TOET20'ST250660

FIG. 1

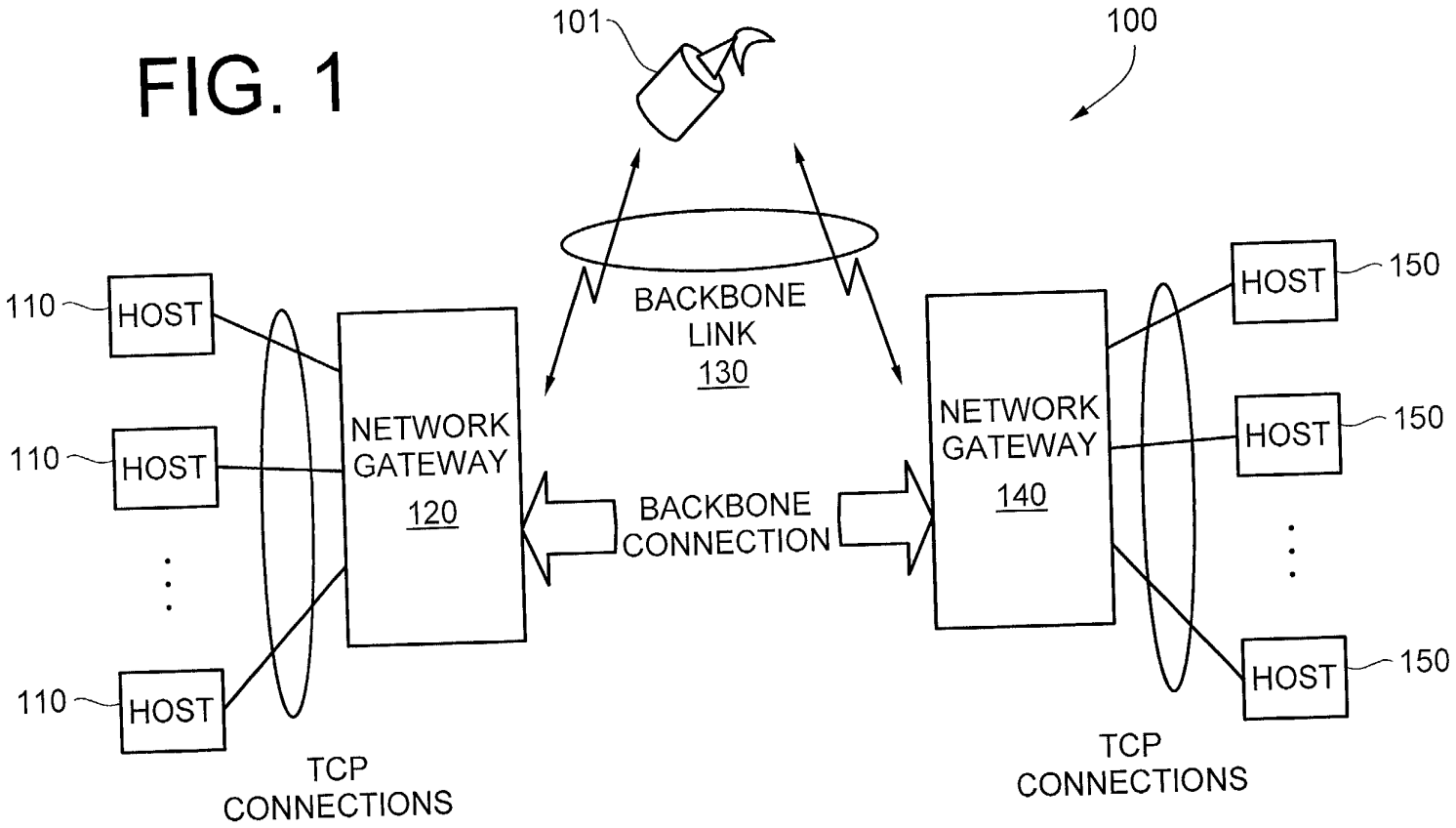


FIG. 2

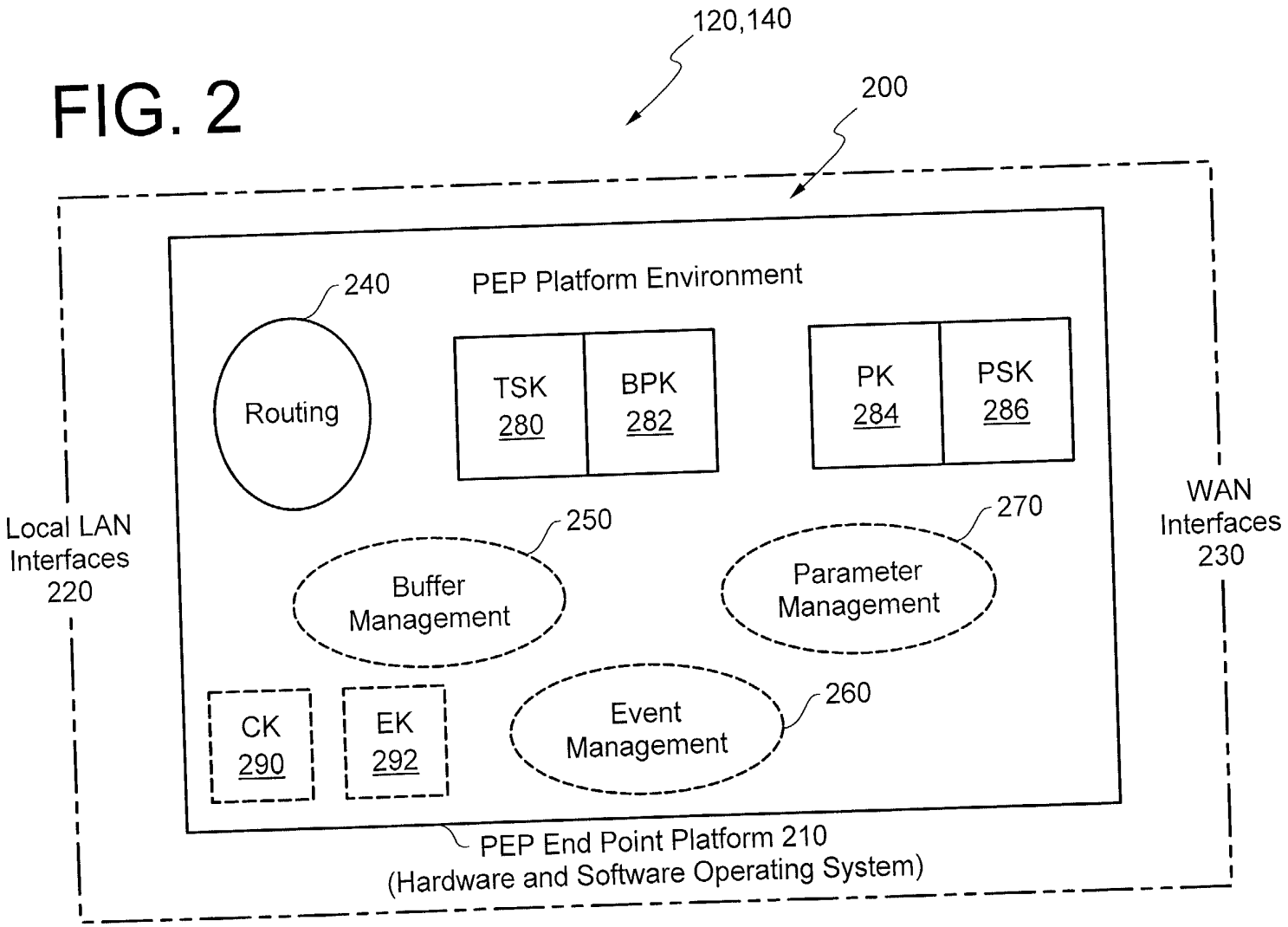
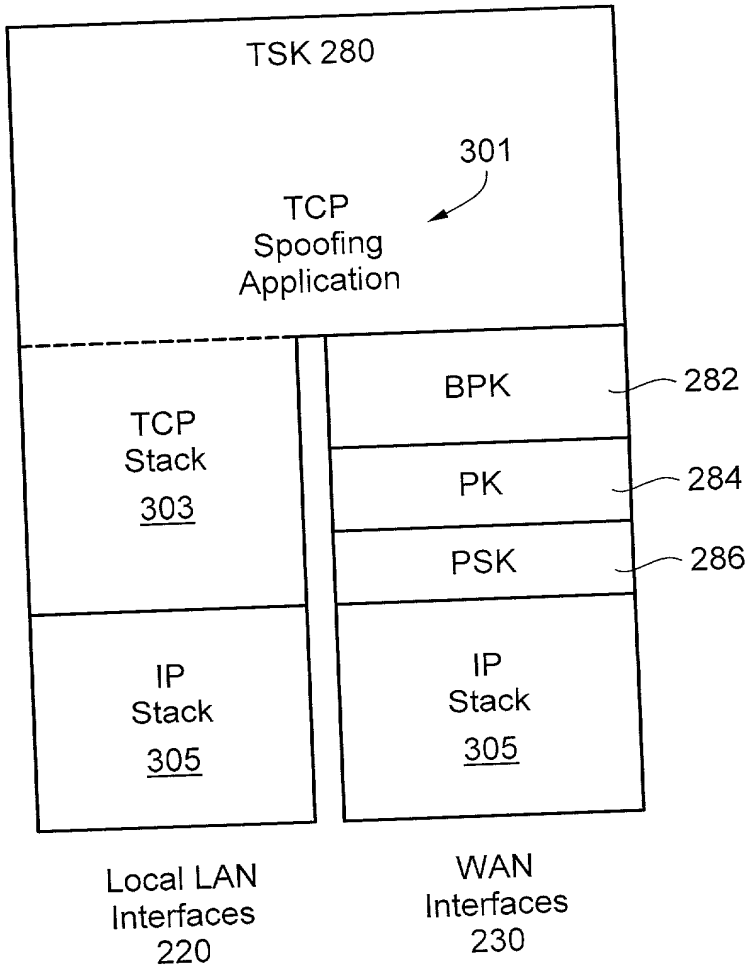

120,140
200
PEP Platform Environment
240
Routing
TSK
280
BPK
282
PK
284
PSK
286
250
Buffer
Management
270
Parameter
Management
CK
290
EK
292
Event
Management
260
Local LAN
Interfaces
220
WAN
Interfaces
230
PEP End Point Platform 210
(Hardware and Software Operating System)

FIG. 3


TSK 280
301
TCP
Spoofing
Application
TCP
Stack
303
BPK
282
PK
284
PSK
286
IP
Stack
305
IP
Stack
305
Local LAN
Interfaces
220
WAN
Interfaces
230

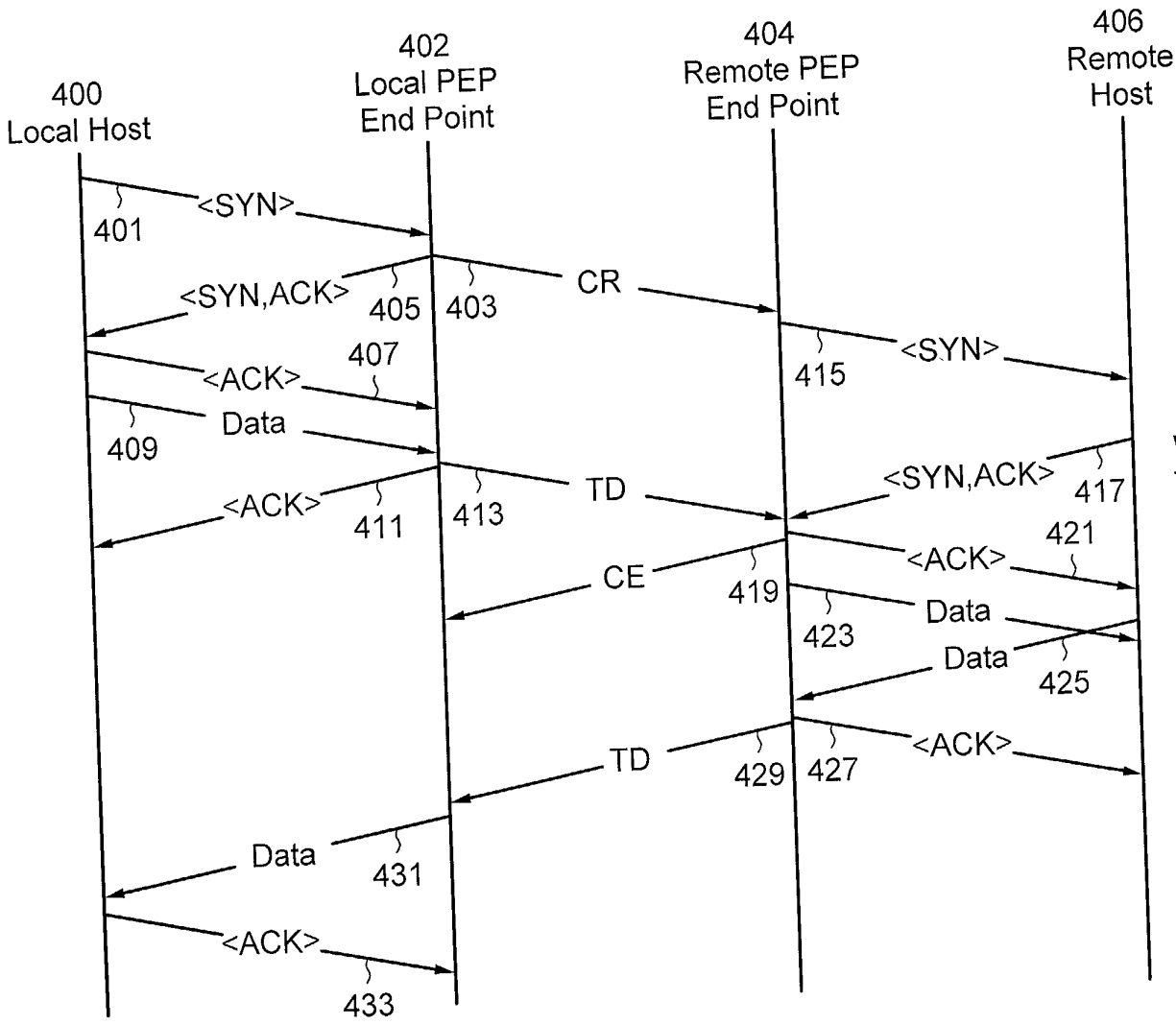

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<SYN>
401
<SYN,ACK>
405
403
CR
<SYN>
415
<ACK>
407
Data
409
<SYN,ACK>
417
With
Three-Way
Handshake
Spoofing
<ACK>
411
413
TD
421
<ACK>
CE
419
Data
423
Data
425
TD
429
427
<ACK>
Data
431
<ACK>
433

FIG. 4A

T0ET20" ST250660

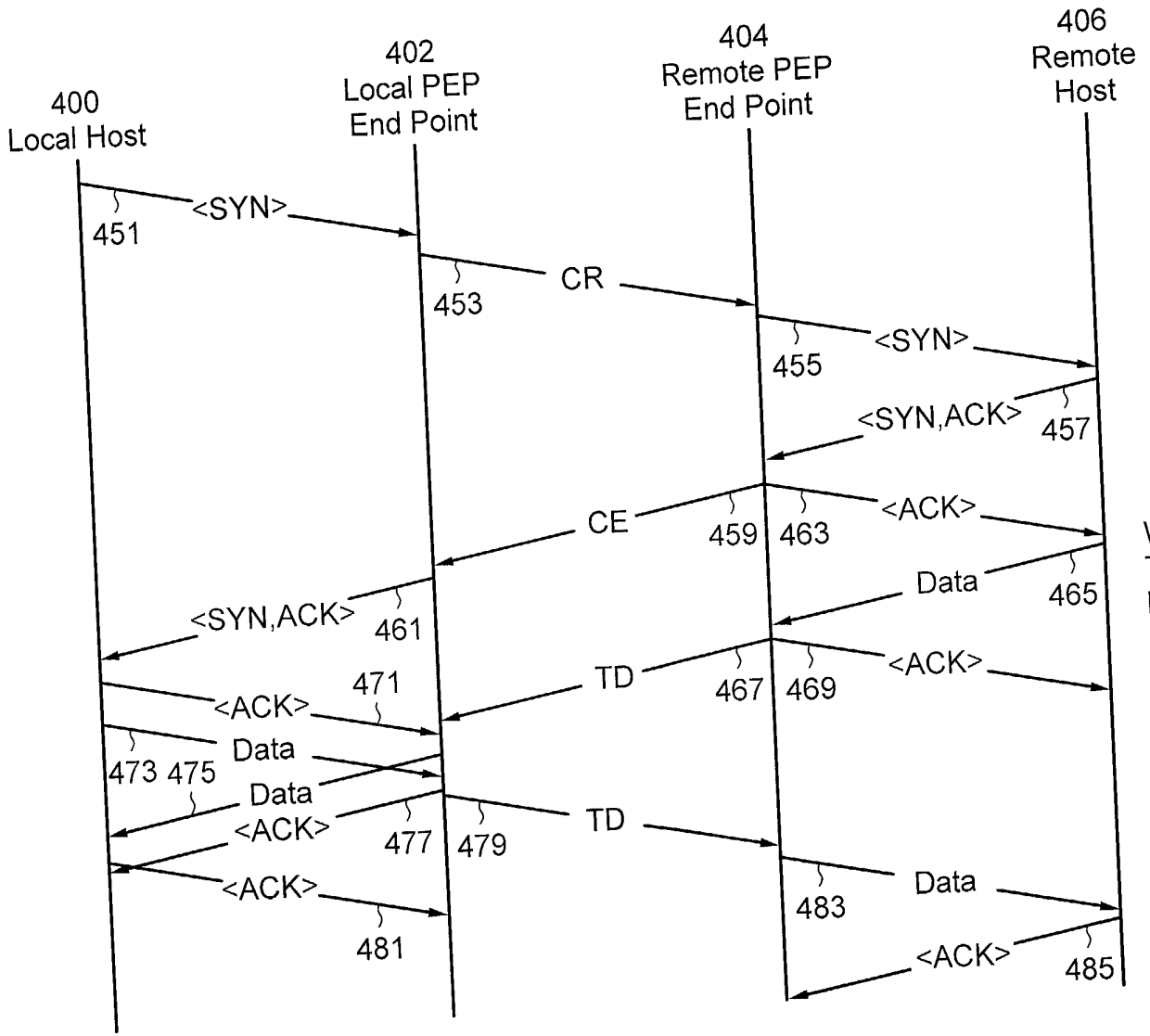


FIG. 4B

TOETZ0 ST250660

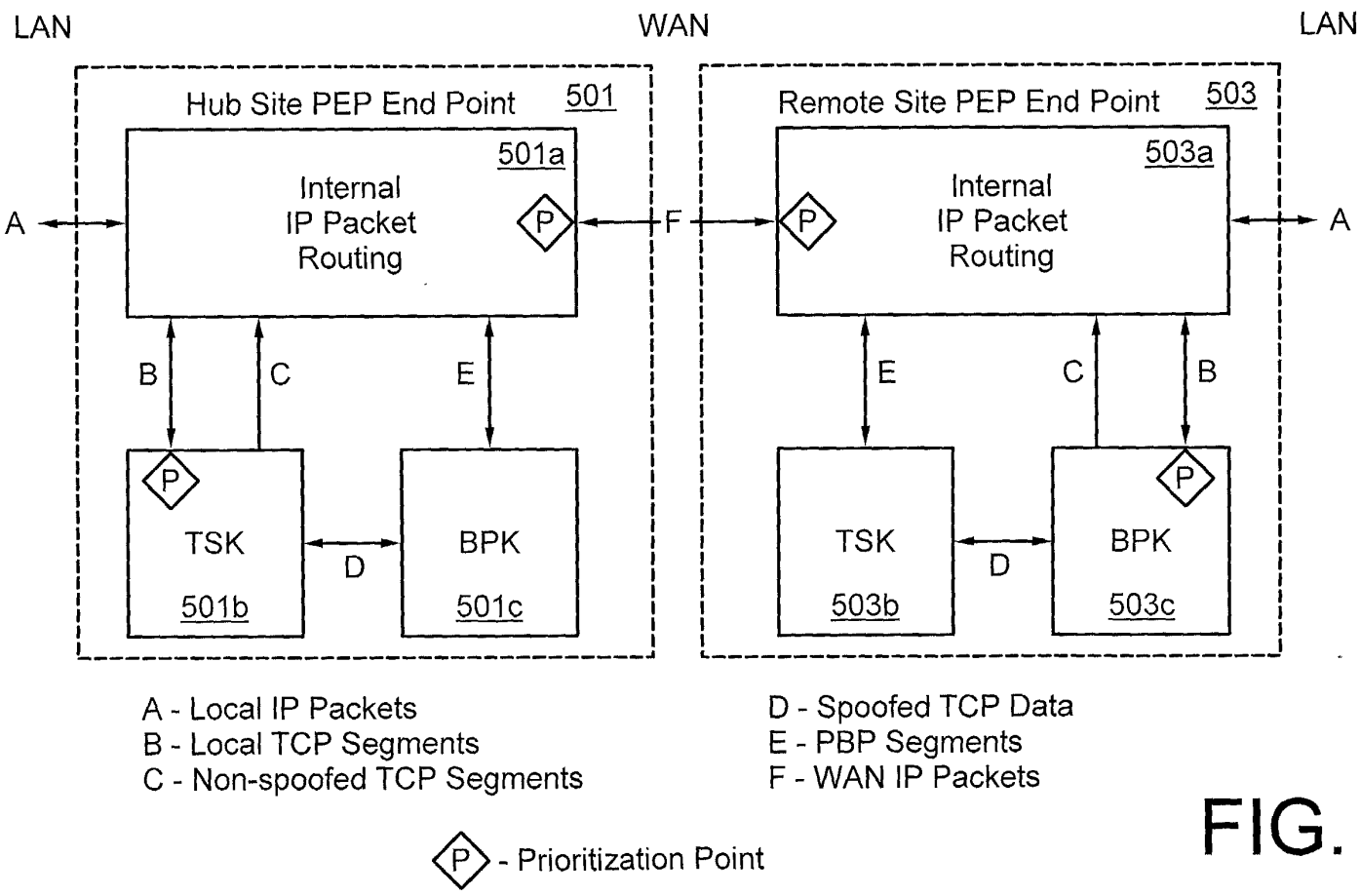


FIG. 5

TOET20" ST2S0660

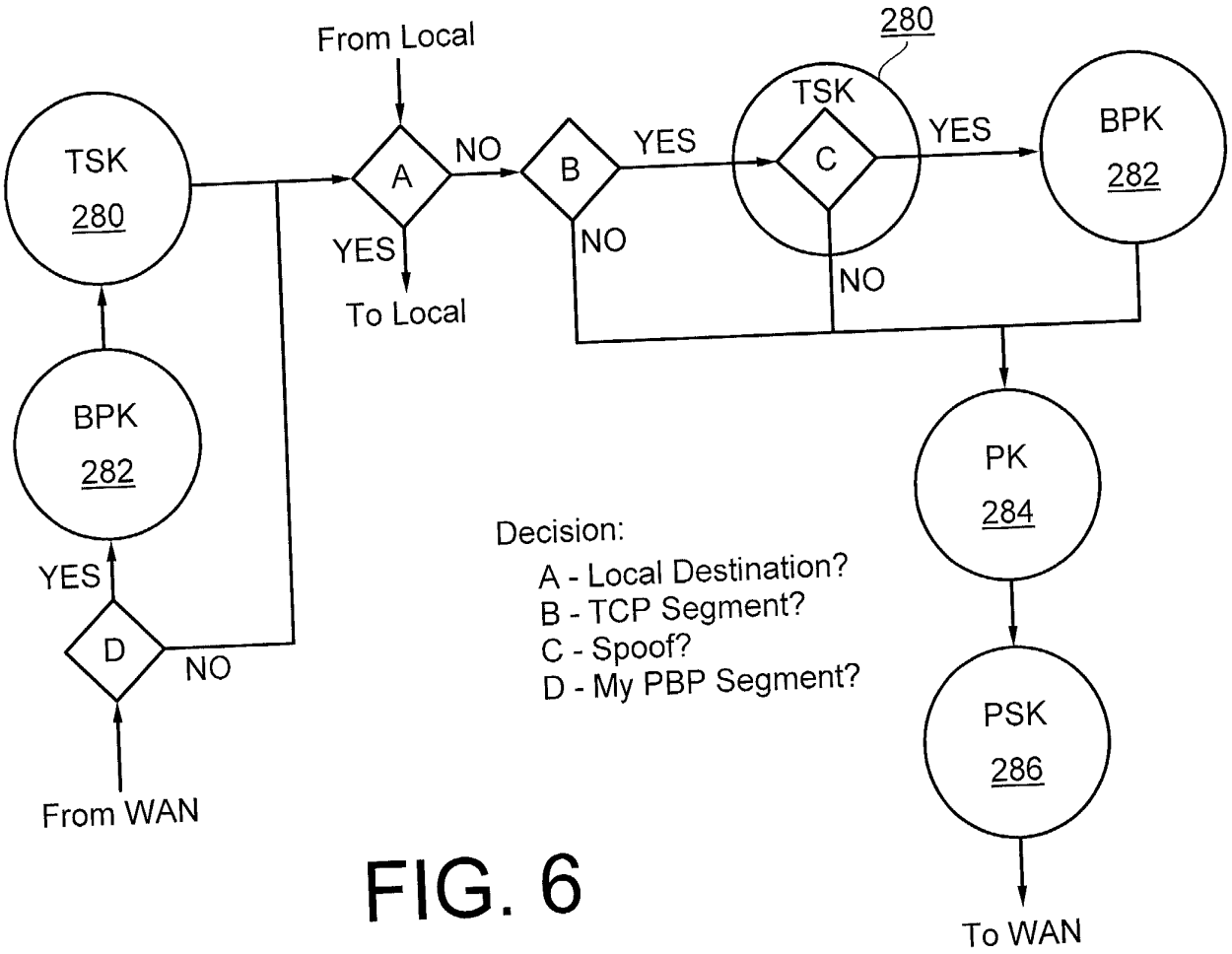


FIG. 6

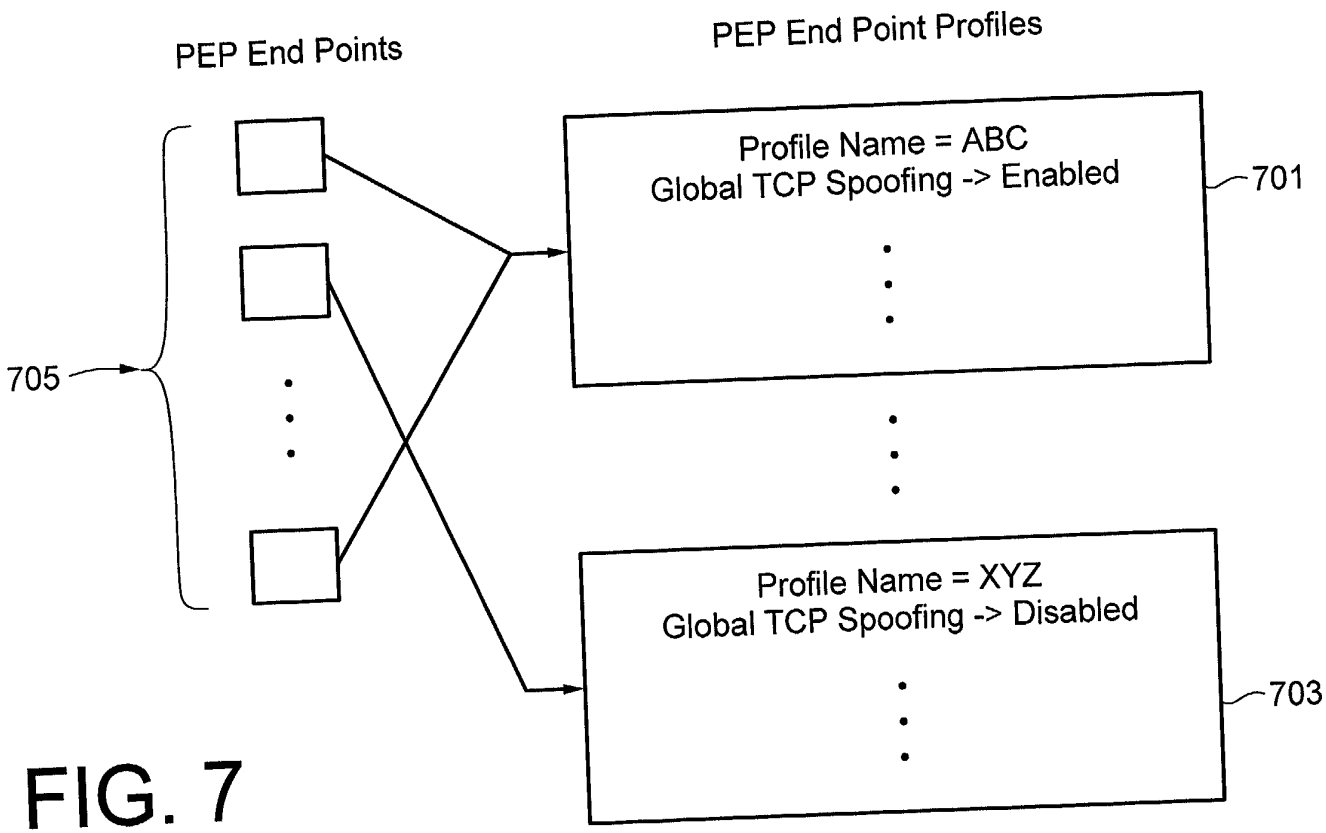

PEP End Points
PEP End Point Profiles
Profile Name = ABC
Global TCP Spoofing -> Enabled
701
705
Profile Name = XYZ
Global TCP Spoofing -> Disabled
703

FIG. 7

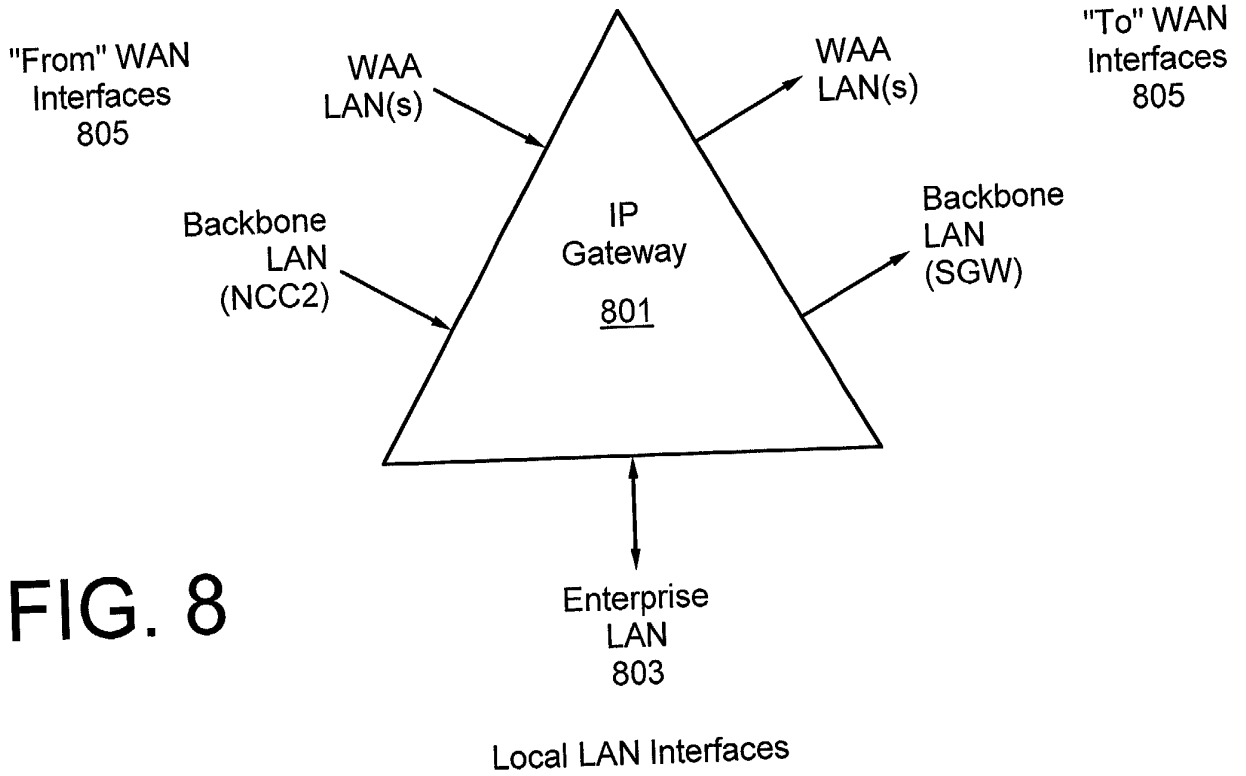

"From" WAN Interfaces 805
WAA LAN(s)
WAA LAN(s)
"To" WAN Interfaces 805
Backbone LAN (NCC2)
IP Gateway
801
Backbone LAN (SGW)
Enterprise LAN 803
Local LAN Interfaces

FIG. 8

TOETZO" ST2S0660

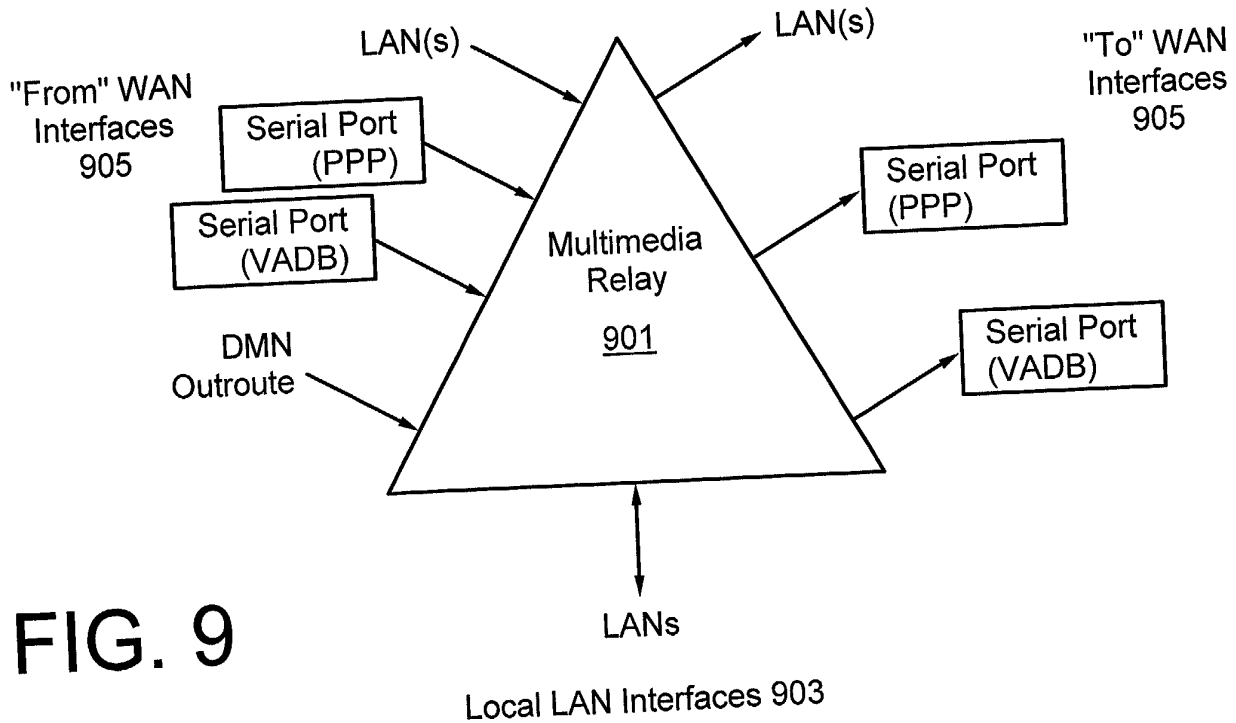


FIG. 9

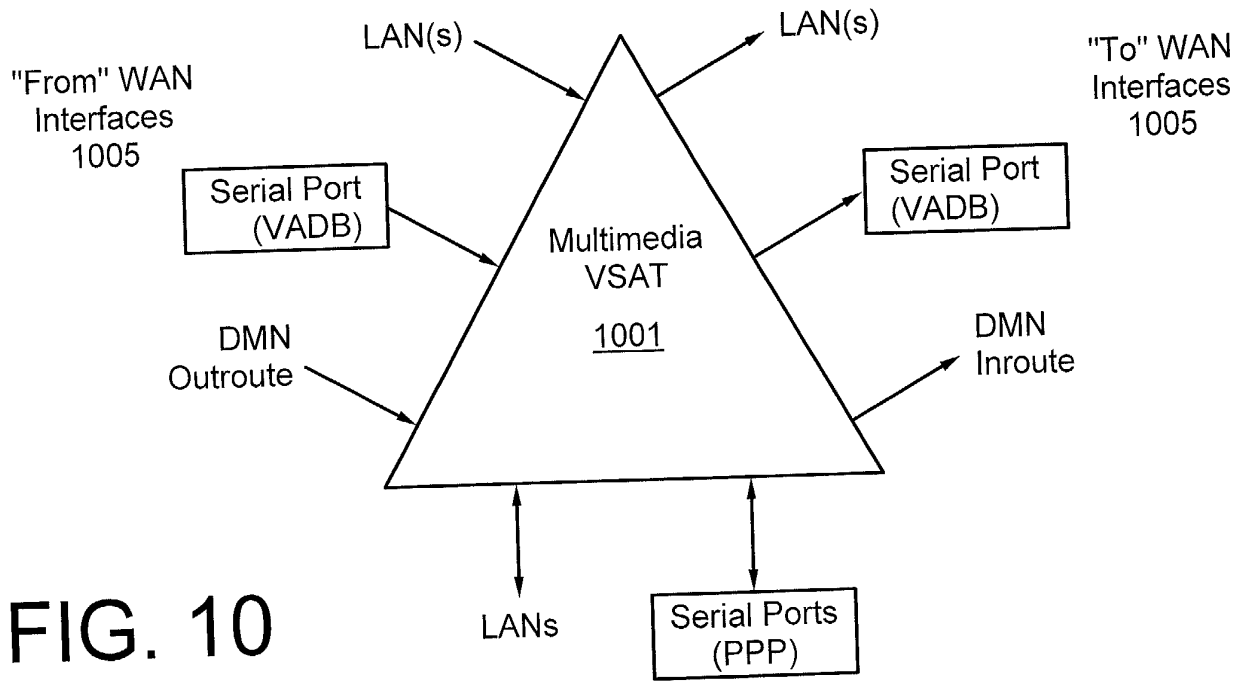

LAN(s)
LAN(s)
"From" WAN Interfaces 1005
"To" WAN Interfaces 1005
Serial Port (VADB)
Serial Port (VADB)
Multimedia VSAT
1001
DMN Outroute
DMN Inroute
LANs
Serial Ports (PPP)
Local LAN Interfaces 1003

FIG. 10

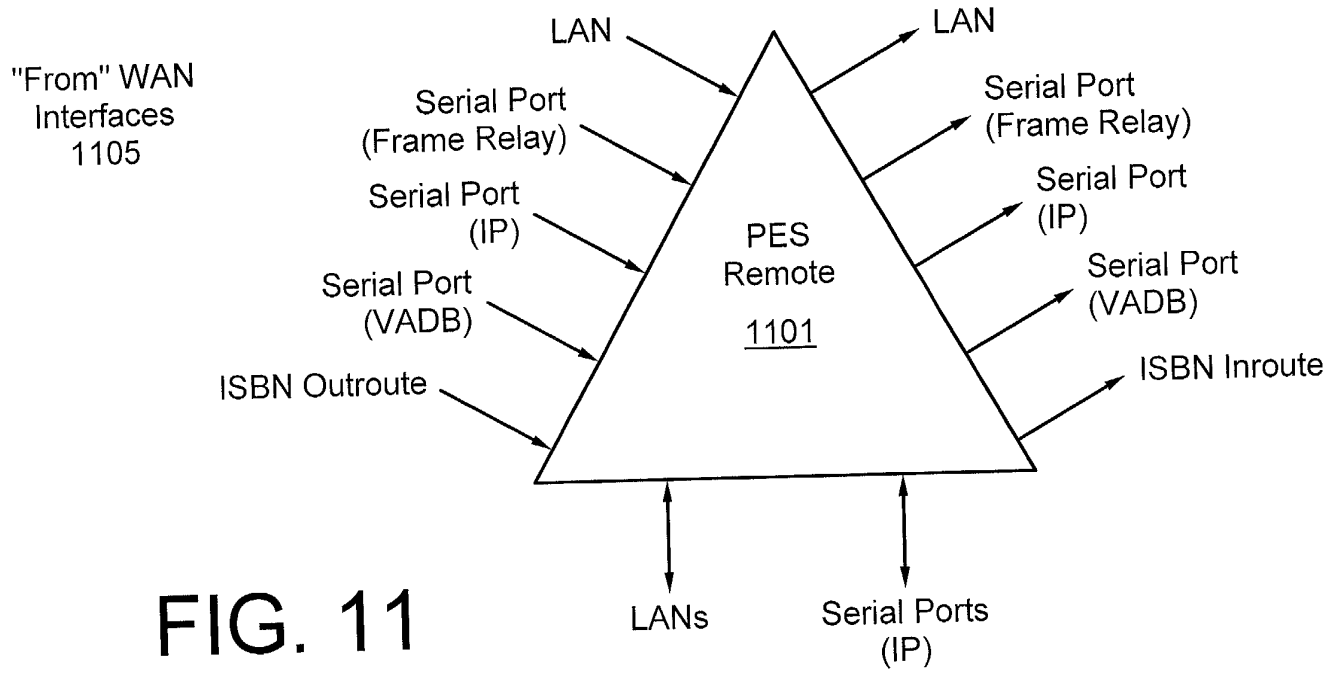
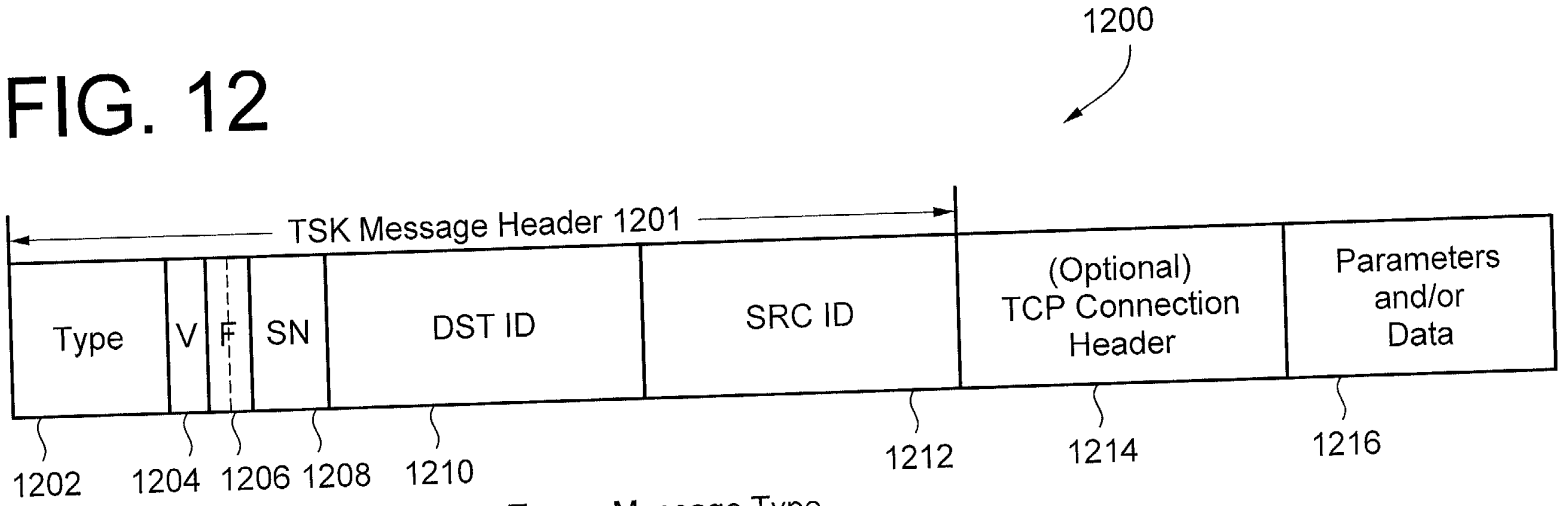

"From" WAN Interfaces 1105
LAN
Serial Port (Frame Relay)
Serial Port (IP)
Serial Port (VADB)
ISBN Outroute
PES Remote
1101
LAN
Serial Port (Frame Relay)
Serial Port (IP)
Serial Port (VADB)
ISBN Inroute
"To" WAN Interfaces 1105
LANs
Serial Ports (IP)
Local LAN Interfaces 1103

FIG. 11

FOETZO ST2S0660

FIG. 12



Type - Message Type
V - Version
F - Flags
SN - Sequence Number
DST ID - Destination Connection Identifier
SRC ID - Source Connection Identifier

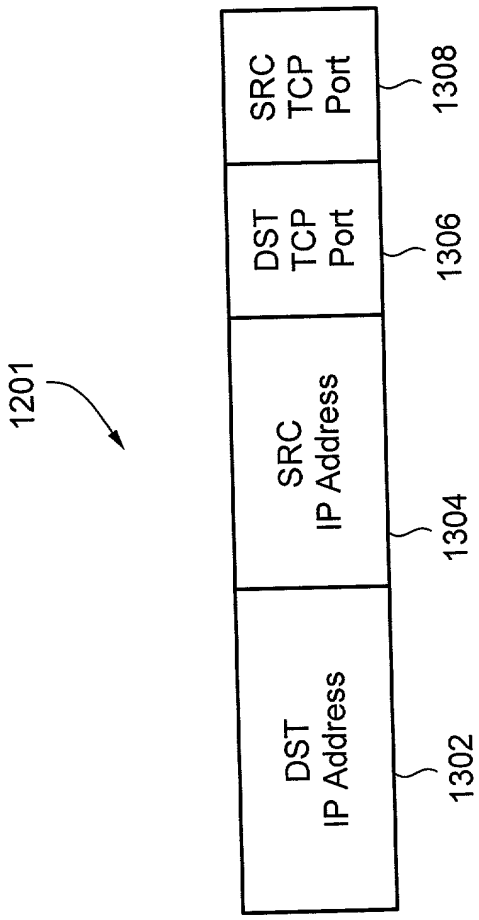
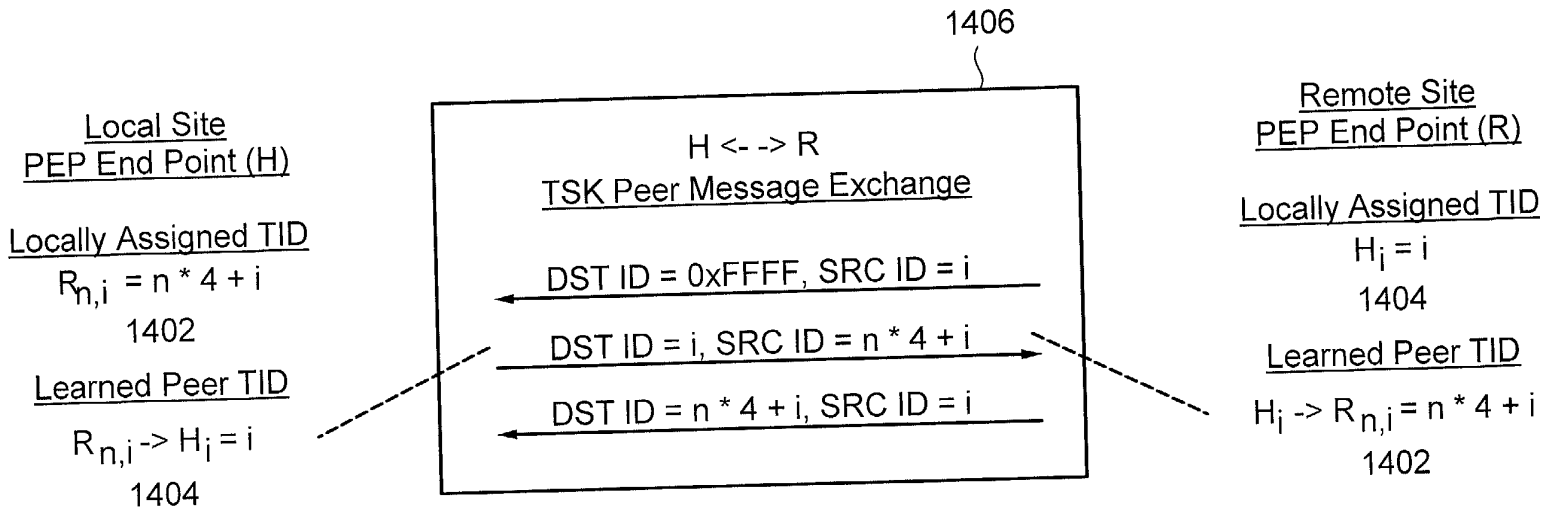

1201
DST IP Address
1302
SRC IP Address
1304
DST TCP Port
1306
SRC TCP Port
1308

FIG. 13



KEY:
n = Peer Index
i = Priority

FIG. 14

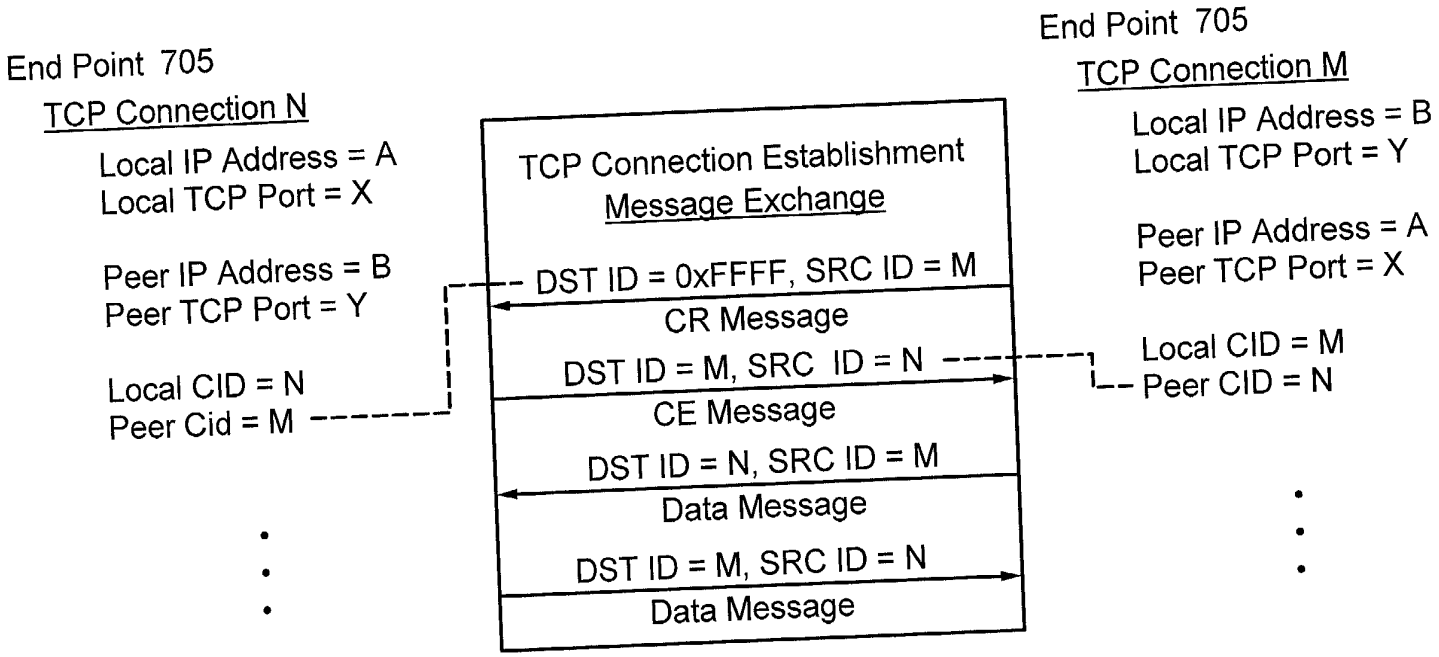

End Point 705
TCP Connection N
Local IP Address = A
Local TCP Port = X
Peer IP Address = B
Peer TCP Port = Y
Local CID = N
Peer Cid = M
TCP Connection Establishment
Message Exchange
DST ID = 0xFFFF, SRC ID = M
CR Message
DST ID = M, SRC ID = N
CE Message
DST ID = N, SRC ID = M
Data Message
DST ID = M, SRC ID = N
Data Message
End Point 705
TCP Connection M
Local IP Address = B
Local TCP Port = Y
Peer IP Address = A
Peer TCP Port = X
Local CID = M
Peer CID = N

FIG. 15

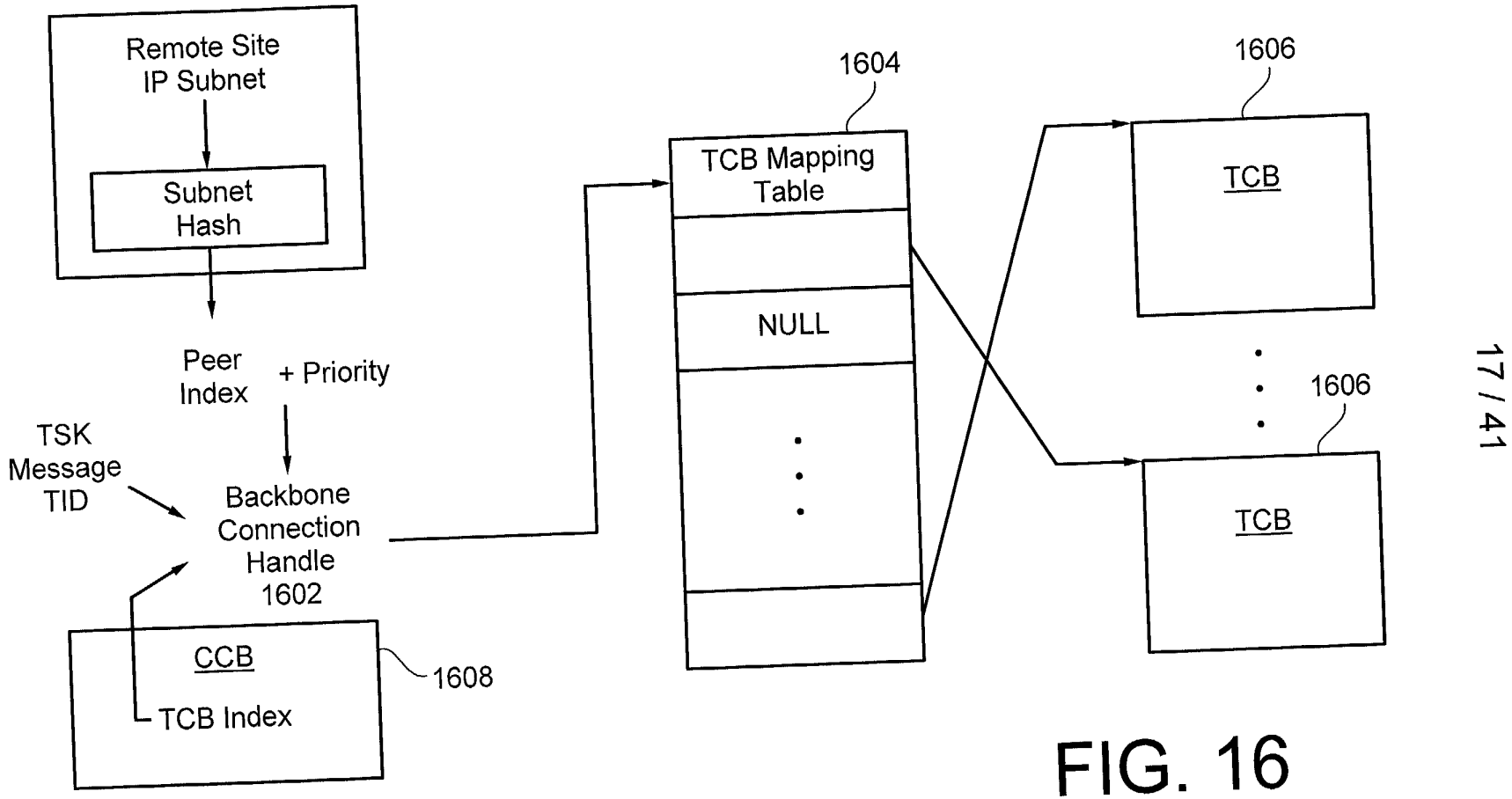

Remote Site
IP Subnet
Subnet
Hash
Peer
Index
+ Priority
TSK
Message
TID
Backbone
Connection
Handle
1602
CCB
TCB Index
1608
1604
TCB Mapping
Table
NULL
1606
TCB
1606
TCB

FIG. 16

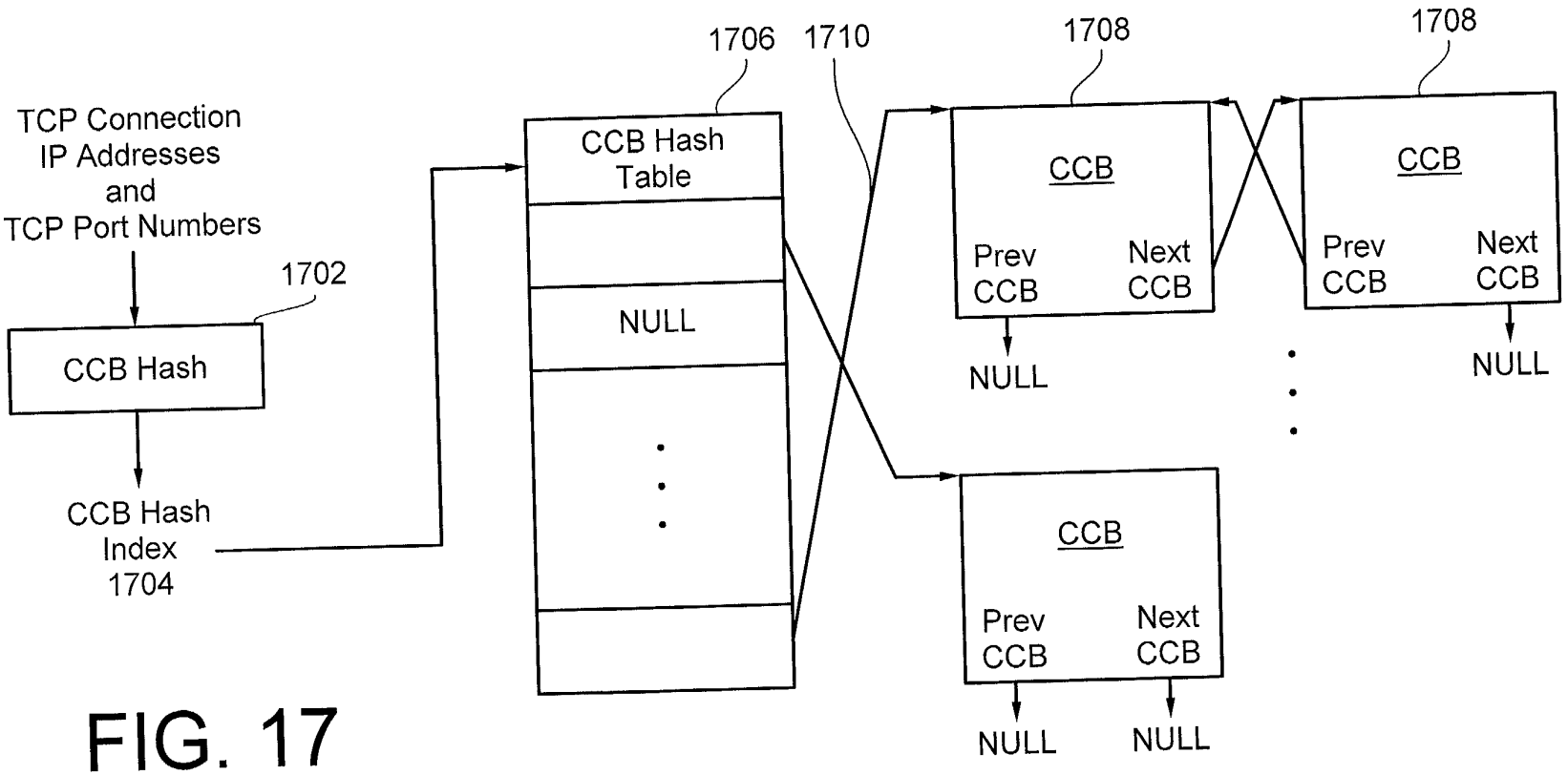
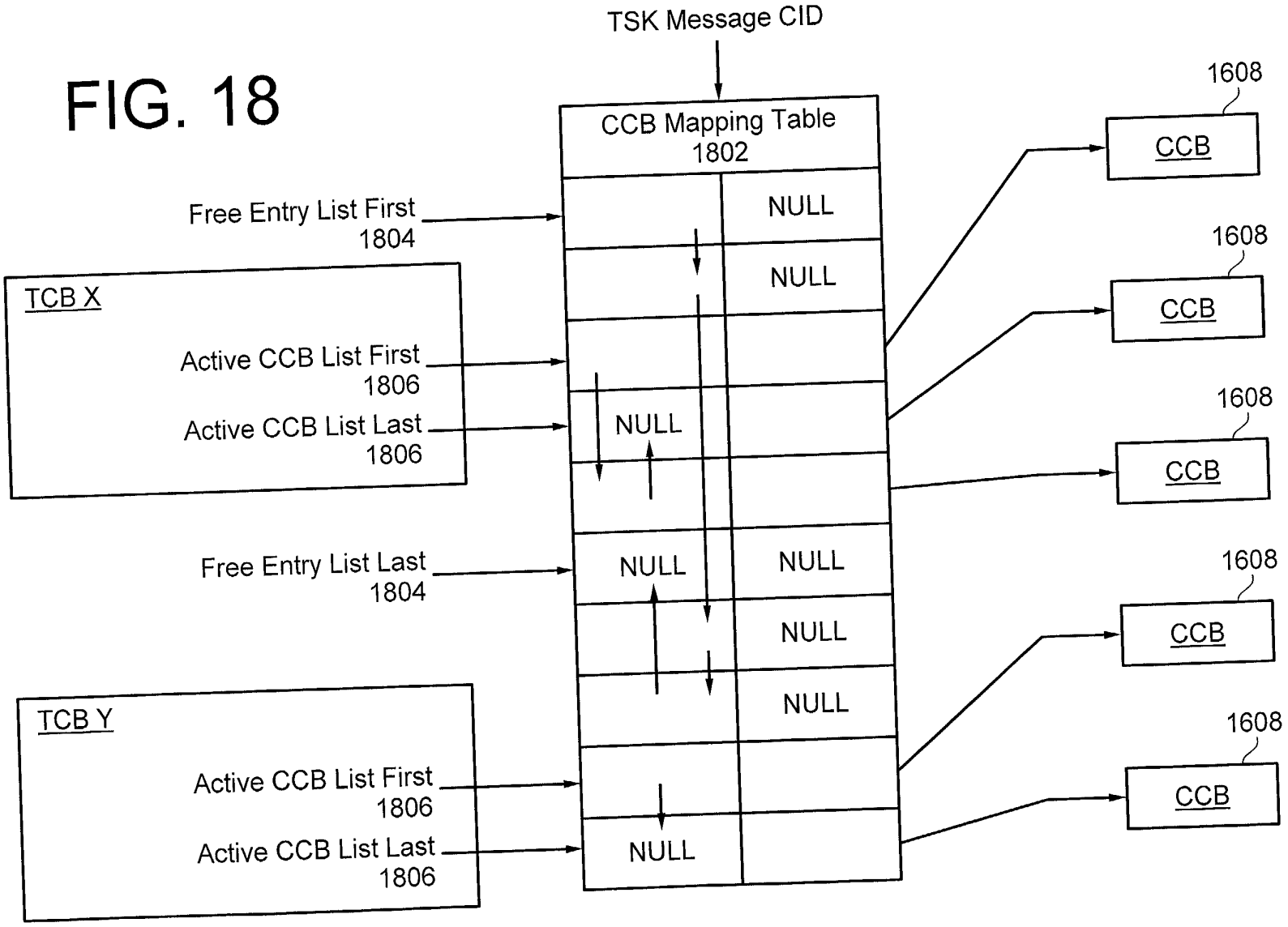

TCP Connection
IP Addresses
and
TCP Port Numbers
1702
CCB Hash
CCB Hash
Index
1704
1706
1710
CCB Hash
Table
NULL
1708
CCB
Prev
CCB
Next
CCB
NULL
1708
CCB
Prev
CCB
Next
CCB
NULL
CCB
Prev
CCB
Next
CCB
NULL
NULL

FIG. 17

FIG. 18


TSK Message CID
CCB Mapping Table
1802
Free Entry List First
1804
TCB X
Active CCB List First
1806
Active CCB List Last
1806
Free Entry List Last
1804
TCB Y
Active CCB List First
1806
Active CCB List Last
1806
NULL
1608
CCB

TOETZO" ST2S0660

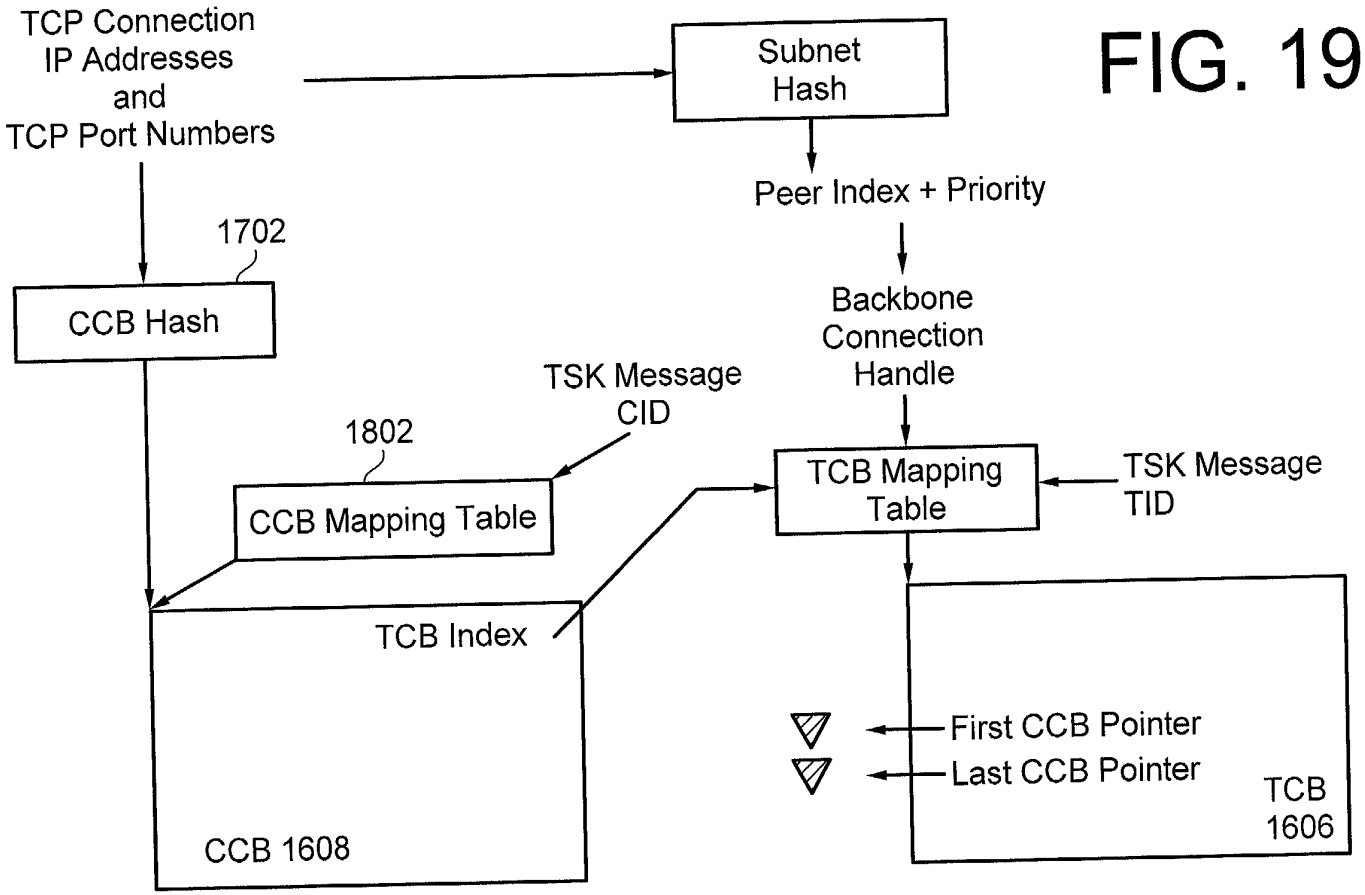
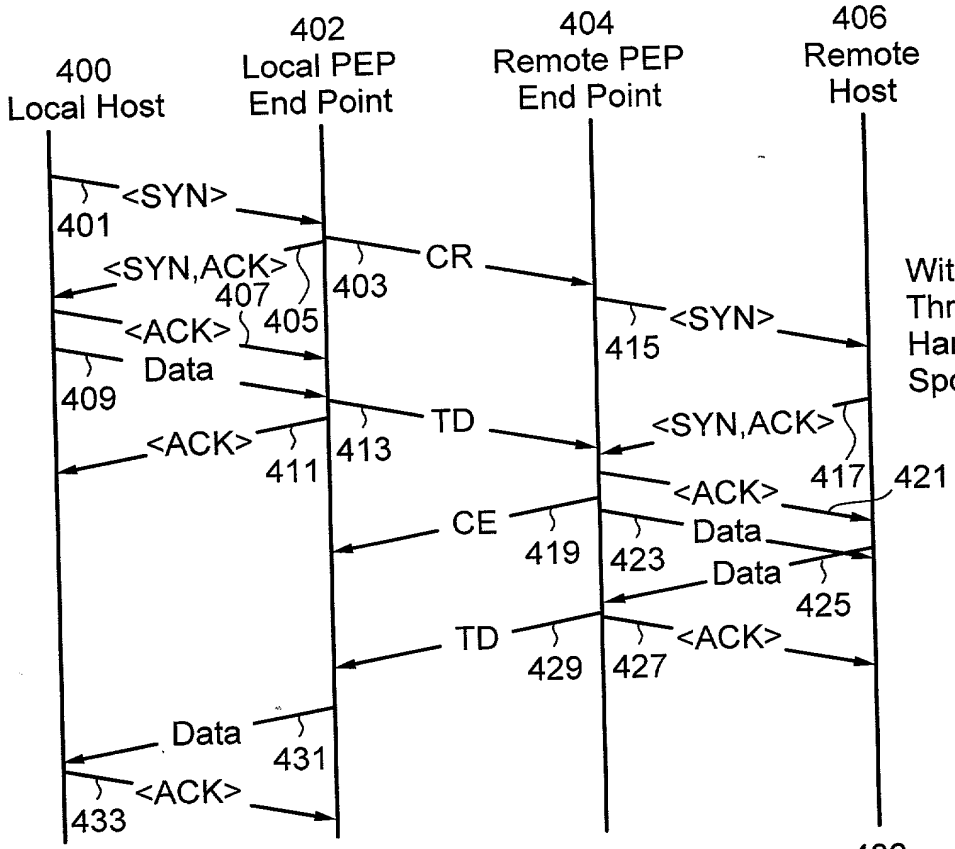


FIG. 19

▽ Points to the CCB via a linked list.


400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<SYN>
401
CR
403
<SYN,ACK>
407
405
<ACK>
Data
409
TD
413
<ACK>
411
<SYN>
415
With
Three-Way
Handshake
Spoofing
<SYN,ACK>
417
421
<ACK>
Data
CE
419
423
Data
425
TD
429
<ACK>
427
Data
431
<ACK>
433

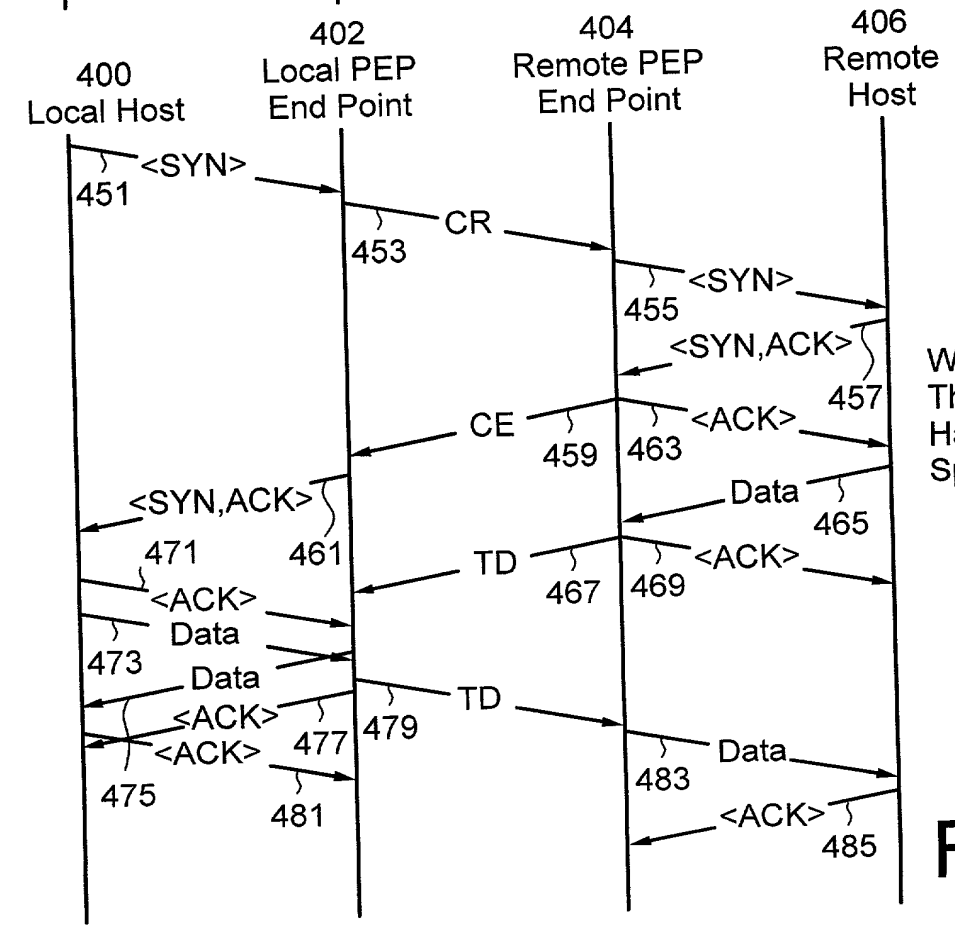

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<SYN>
451
CR
453
<SYN>
455
<SYN,ACK>
457
Without
Three-Way
Handshake
Spoofing
CE
459
<ACK>
463
Data
465
<SYN,ACK>
471
461
TD
467
<ACK>
469
<ACK>
Data
473
Data
<ACK>
TD
<ACK>
475
477
479
Data
483
<ACK>
481
485

FIG. 20

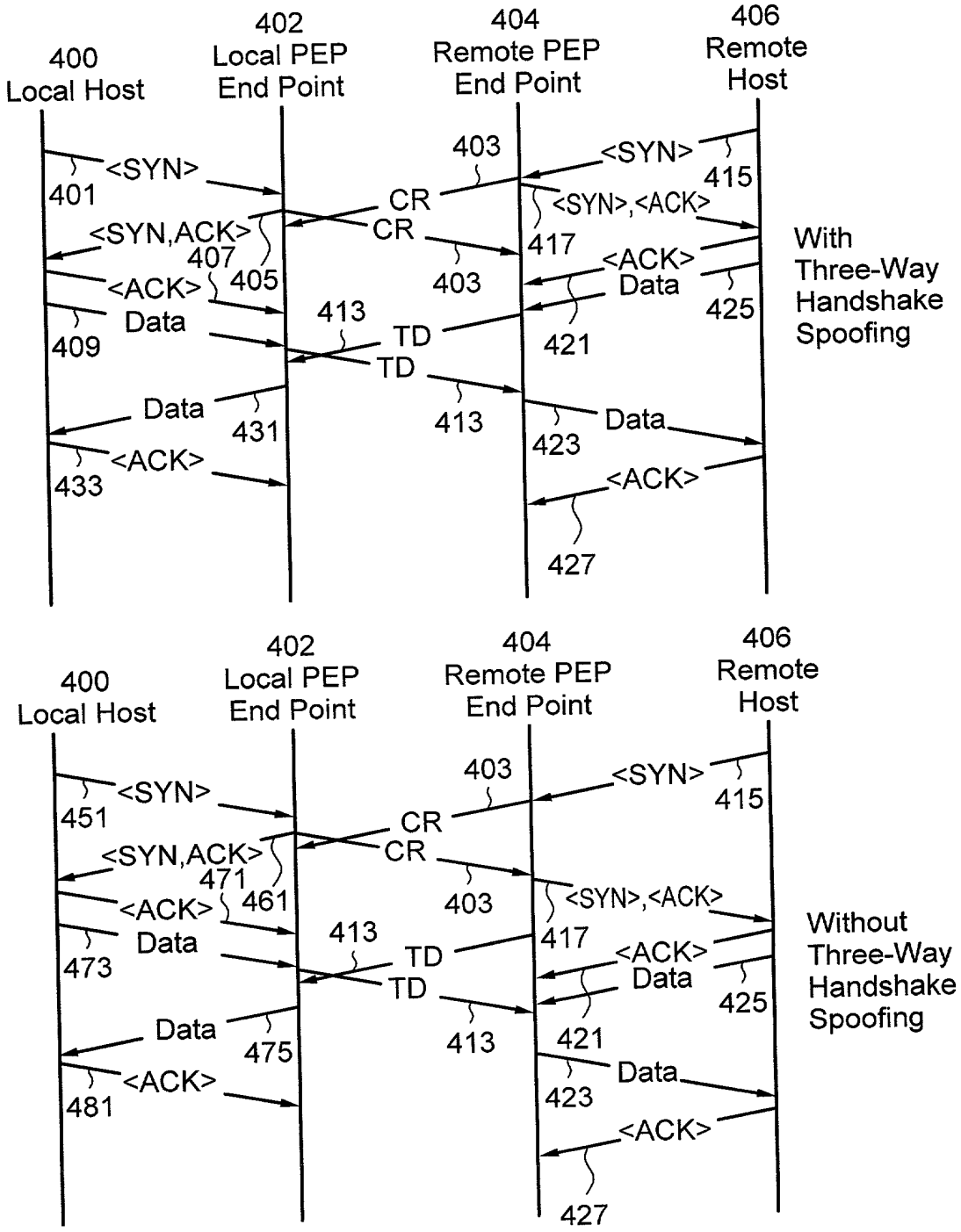

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<SYN>
401
CR
403
<SYN>
403
<SYN>,<ACK>
415
<SYN,ACK>
407
CR
403
417
<ACK>
405
Data
425
With
Three-Way
Handshake
Spoofing
<ACK>
Data
409
413
TD
TD
421
Data
431
413
Data
423
<ACK>
433
<ACK>
427
400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<SYN>
451
CR
403
<SYN>
403
<SYN>,<ACK>
415
<SYN,ACK>
471
CR
403
417
<ACK>
461
Data
425
Without
Three-Way
Handshake
Spoofing
<ACK>
Data
473
413
TD
TD
421
Data
475
413
Data
423
<ACK>
481
<ACK>
427

FIG. 21

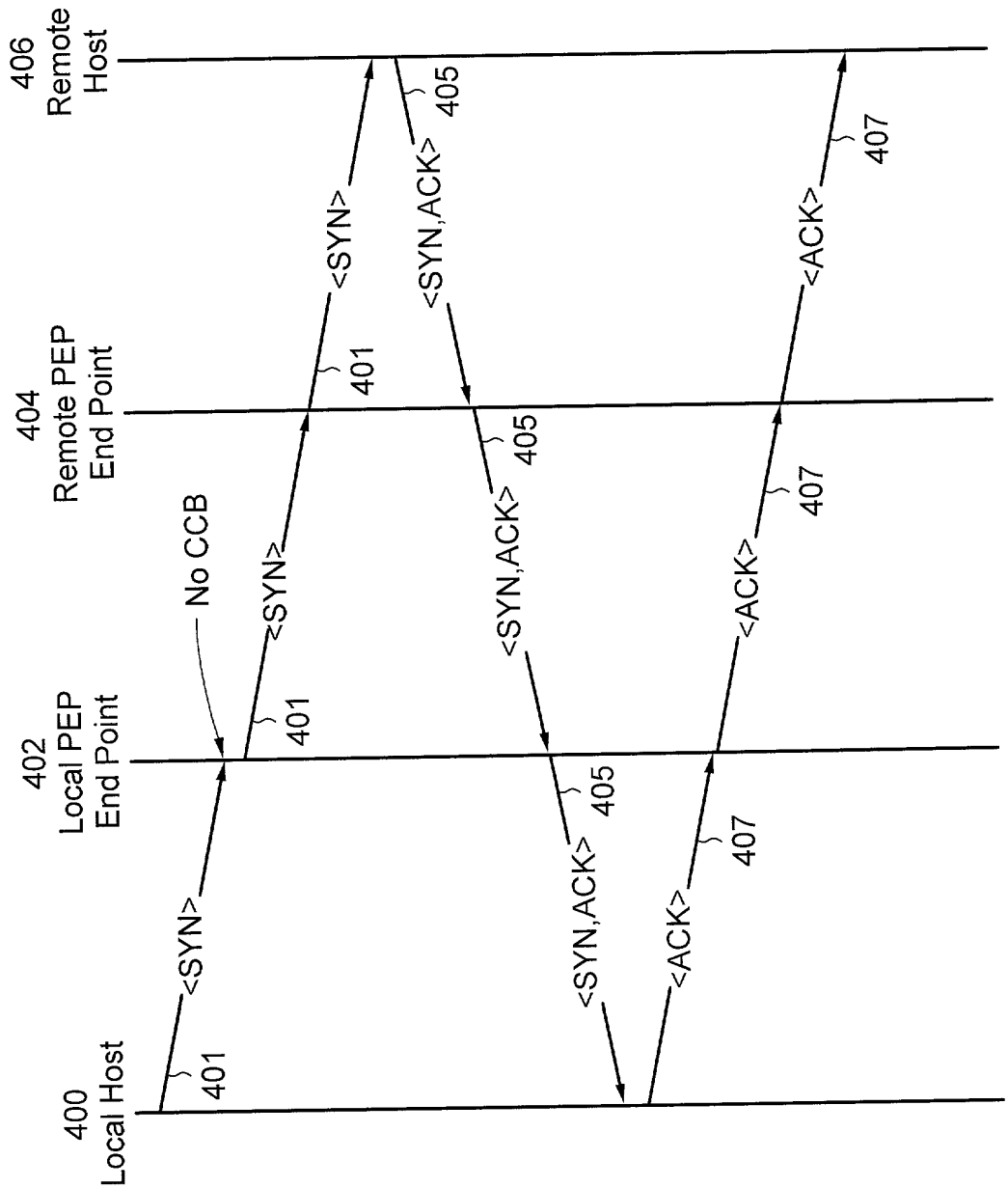

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
No CCB
<SYN>
401
<SYN,ACK>
405
<ACK>
407

FIG. 22

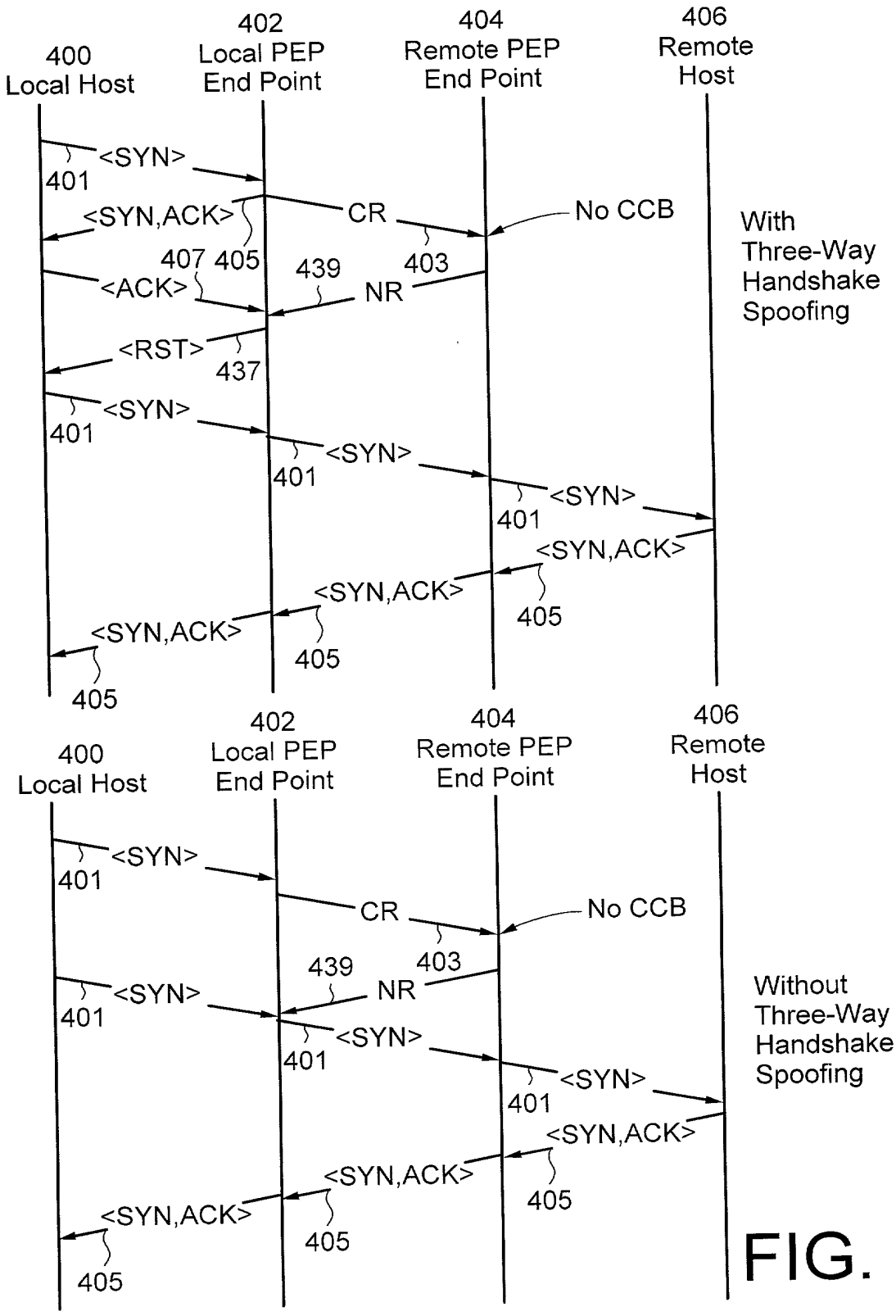
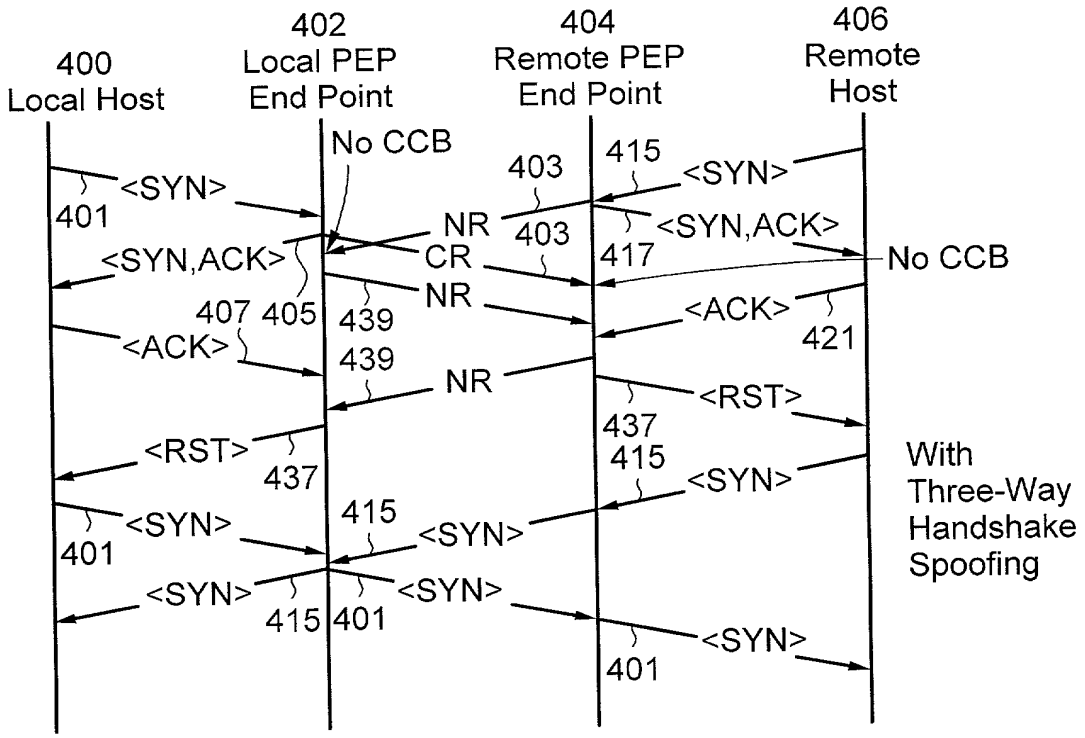

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<SYN>
401
<SYN,ACK>
CR
No CCB
407
405
439
403
<ACK>
NR
With
Three-Way
Handshake
Spoofing
<RST>
437
<SYN>
401
<SYN>
401
<SYN>
401
<SYN,ACK>
<SYN,ACK>
405
<SYN,ACK>
405
405
400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<SYN>
401
CR
No CCB
403
439
NR
<SYN>
401
<SYN>
401
<SYN>
401
Without
Three-Way
Handshake
Spoofing
<SYN,ACK>
<SYN,ACK>
405
<SYN,ACK>
405
405

FIG. 23


400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
No CCB
403
415
<SYN>
401
NR
403
<SYN,ACK>
<SYN,ACK>
CR
417
No CCB
NR
407
405
439
<ACK>
421
<ACK>
439
NR
<RST>
437
<RST>
437
415
With
Three-Way
Handshake
Spoofing
<SYN>
<SYN>
401
415
<SYN>
<SYN>
415
401
<SYN>
401

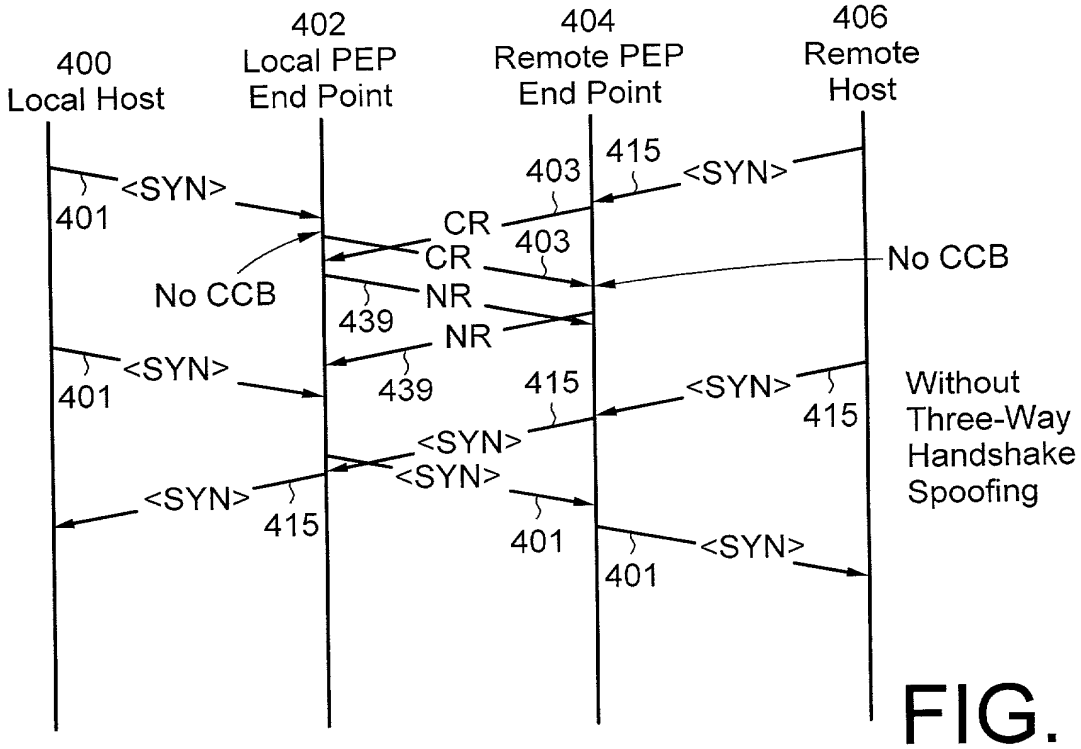

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
403
415
<SYN>
401
CR
403
CR
No CCB
No CCB
NR
439
NR
<SYN>
401
439
415
<SYN>
415
Without
Three-Way
Handshake
Spoofing
<SYN>
<SYN>
<SYN>
415
401
<SYN>
401

FIG. 24

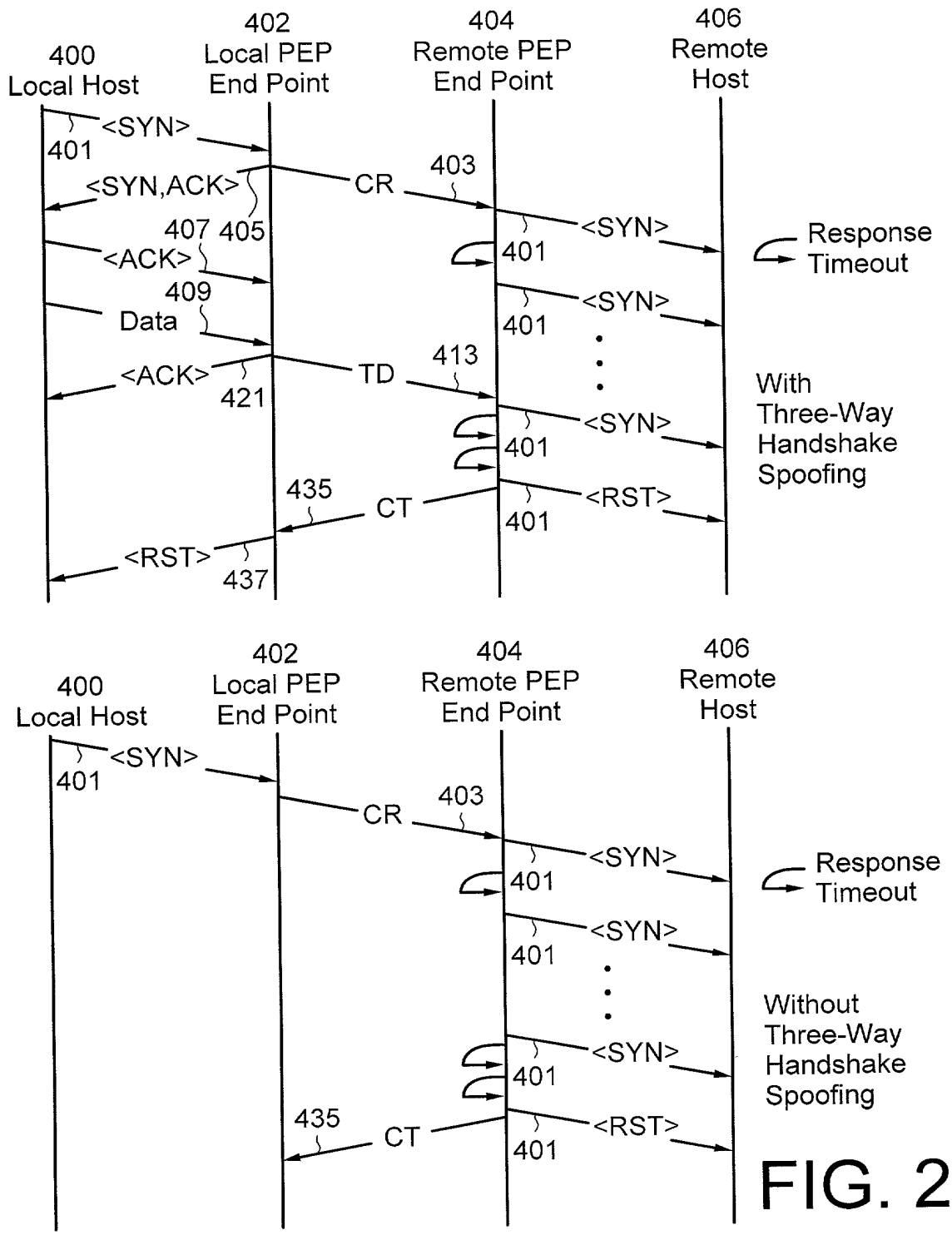

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<SYN>
401
CR
403
<SYN,ACK>
407
405
<SYN>
401
Response
Timeout
<ACK>
409
Data
<SYN>
401
413
TD
<ACK>
421
With
Three-Way
Handshake
Spoofing
<SYN>
401
435
CT
<RST>
401
<RST>
437
400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<SYN>
401
CR
403
<SYN>
401
Response
Timeout
<SYN>
401
Without
Three-Way
Handshake
Spoofing
<SYN>
401
435
CT
<RST>
401

FIG. 25

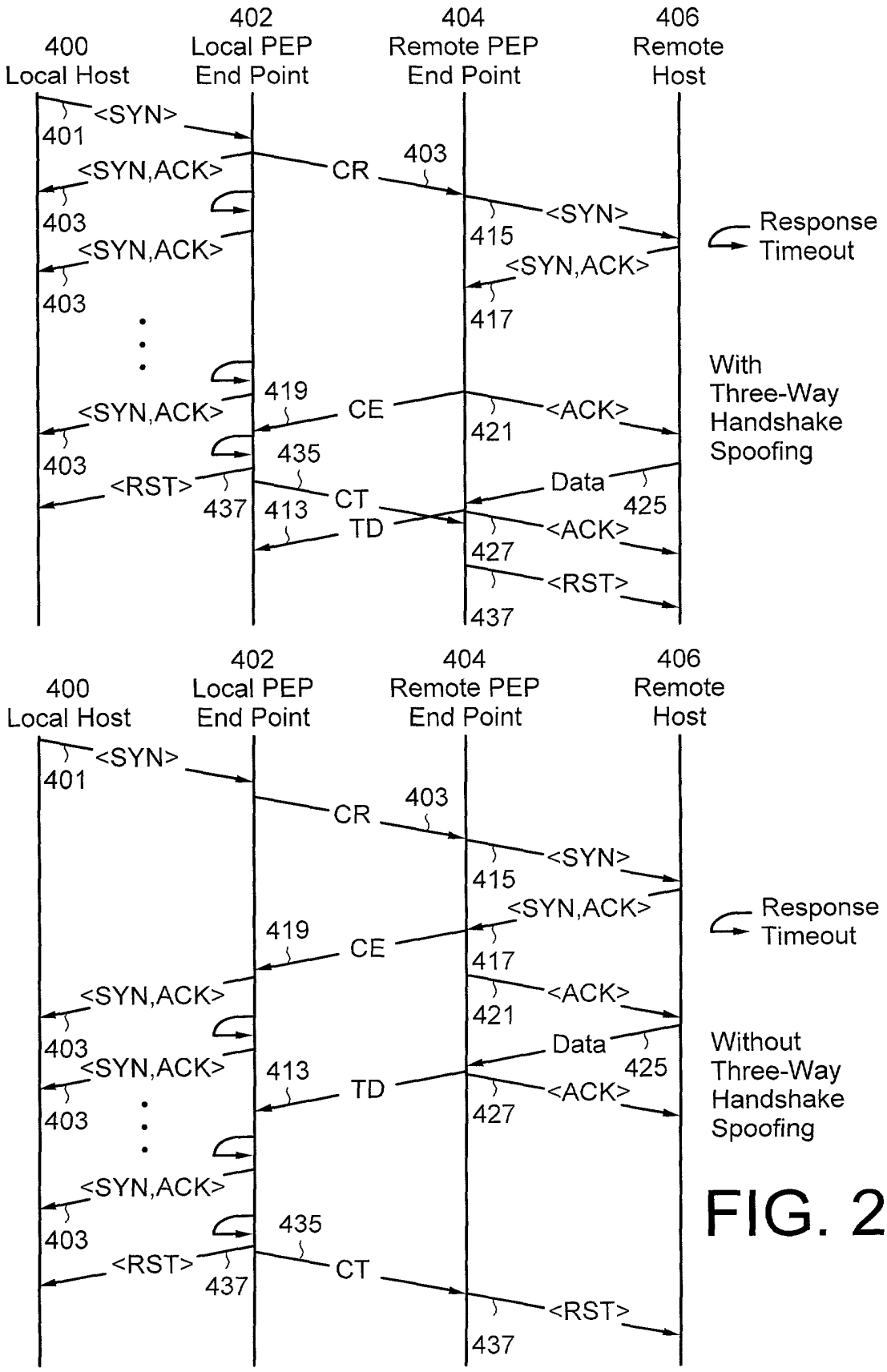

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<SYN>
401
CR
403
<SYN,ACK>
403
<SYN>
415
Response
Timeout
<SYN,ACK>
417
<SYN,ACK>
403
With
Three-Way
Handshake
Spoofing
419
CE
<ACK>
421
<SYN,ACK>
403
435
<RST>
437
CT
413
Data
425
TD
<ACK>
427
<RST>
437
400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<SYN>
401
CR
403
<SYN>
415
<SYN,ACK>
Response
Timeout
419
CE
417
<SYN,ACK>
<ACK>
403
421
Data
<SYN,ACK>
413
425
Without
Three-Way
Handshake
Spoofing
403
TD
<ACK>
427
<SYN,ACK>
403
435
<RST>
437
CT
<RST>
437

FIG. 26

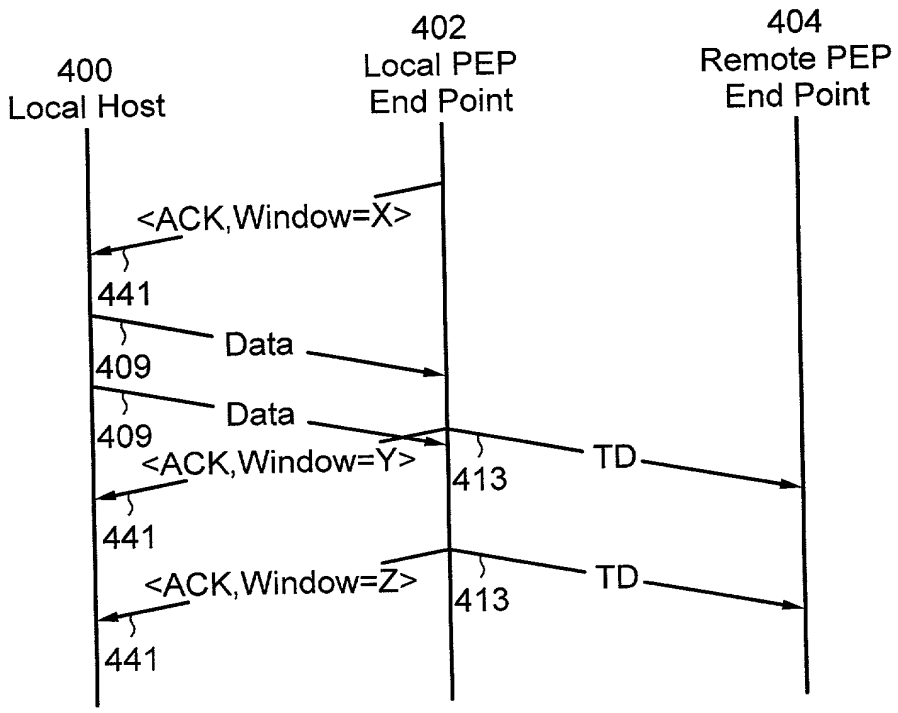

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
<ACK,Window=X>
441
Data
409
Data
409
<ACK,Window=Y>
441
413
TD
<ACK,Window=Z>
441
413
TD

FIG. 27

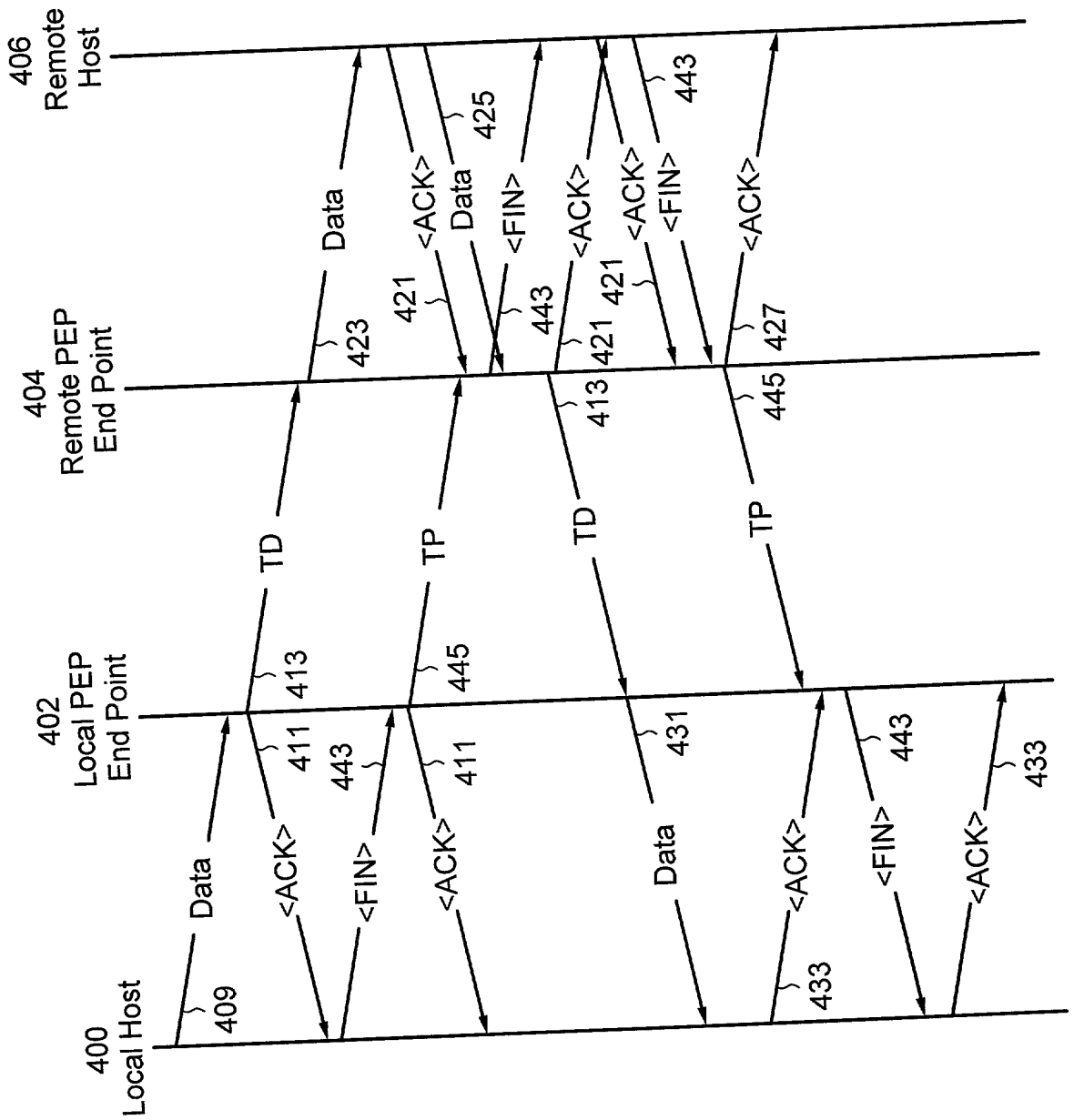

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
Data
409
<ACK>
411
<FIN>
443
<ACK>
411
TD
413
TP
445
Data
423
<ACK>
421
Data
425
<FIN>
443
TD
413
<ACK>
421
<ACK>
421
<FIN>
443
TP
445
<ACK>
427
Data
431
<ACK>
433
<FIN>
443
<ACK>
433

FIG. 28

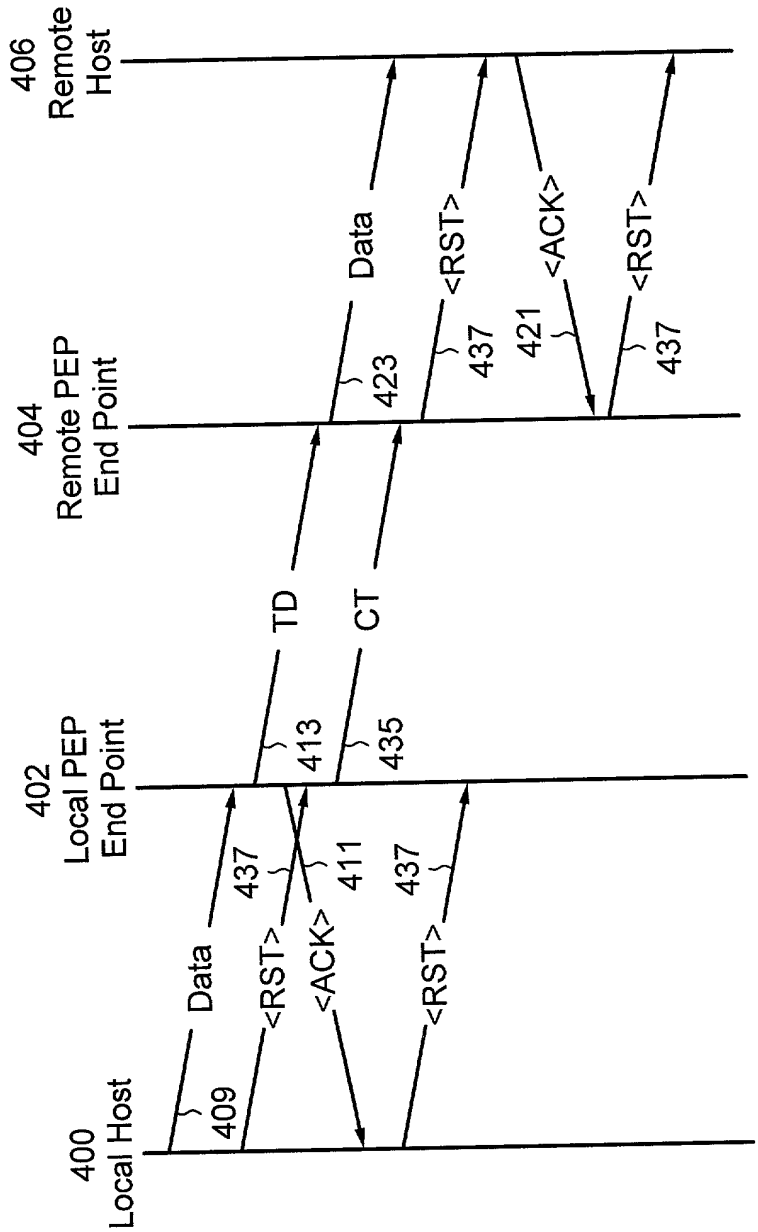

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
Data
409
<RST>
437
<ACK>
411
<RST>
437
TD
413
CT
435
Data
423
<RST>
437
<ACK>
421
<RST>
437

FIG. 29

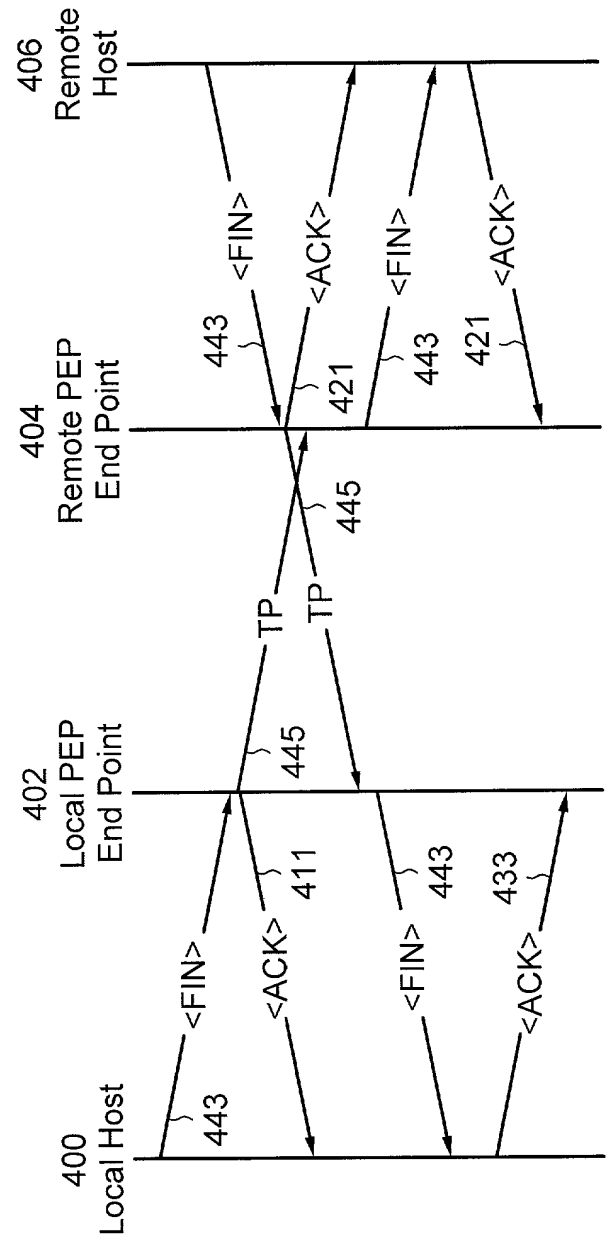

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<FIN>
443
<ACK>
411
<FIN>
443
<ACK>
433
TP
445
TP
445
<FIN>
443
<ACK>
421
<FIN>
443
<ACK>
421

FIG. 30

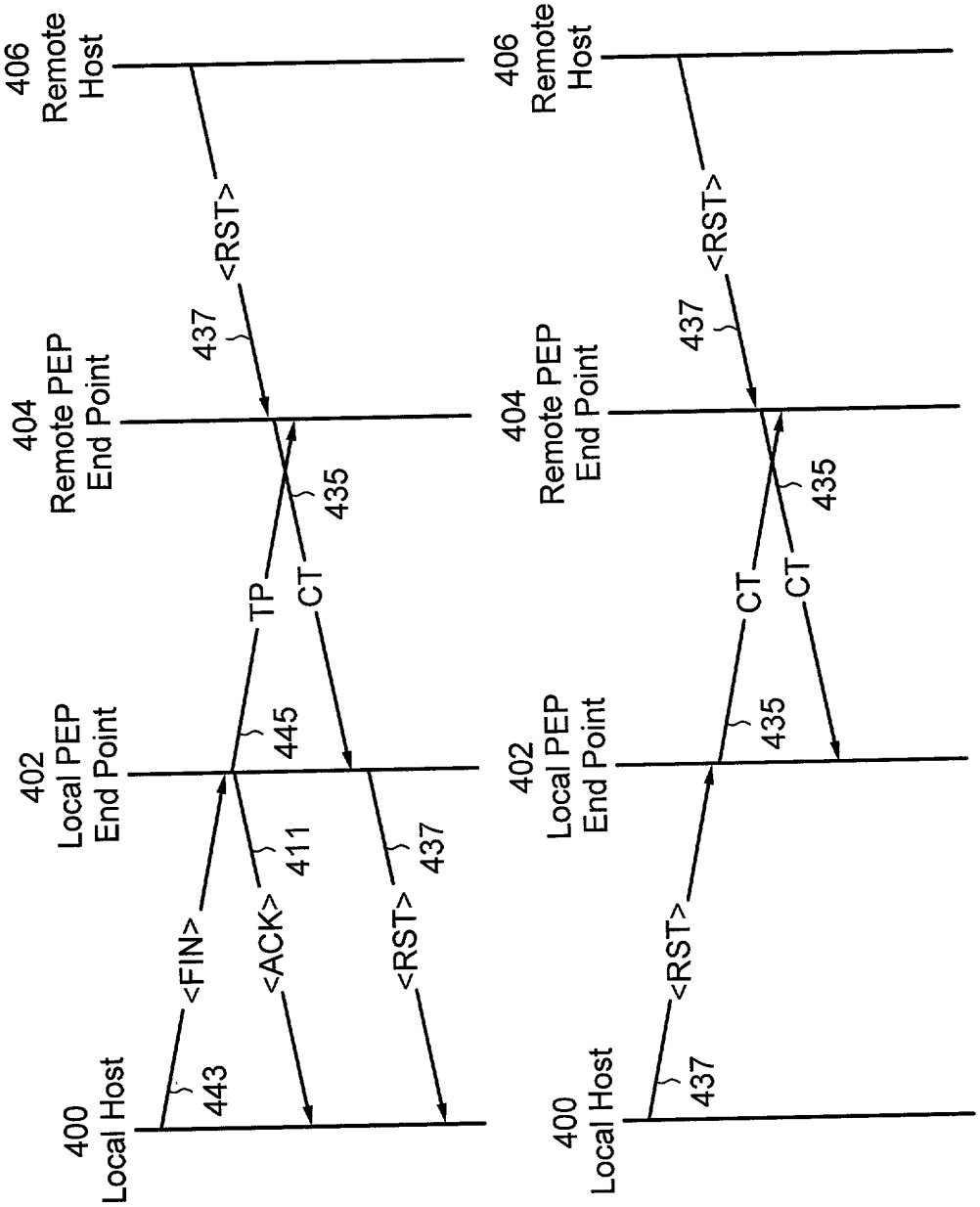

400
Local Host
443
<FIN>
<ACK>
411
<RST>
437
402
Local PEP
End Point
445
TP
CT
435
404
Remote PEP
End Point
437
<RST>
406
Remote
Host
400
Local Host
437
<RST>
402
Local PEP
End Point
435
CT
CT
404
Remote PEP
End Point
437
<RST>
406
Remote
Host

FIG. 31

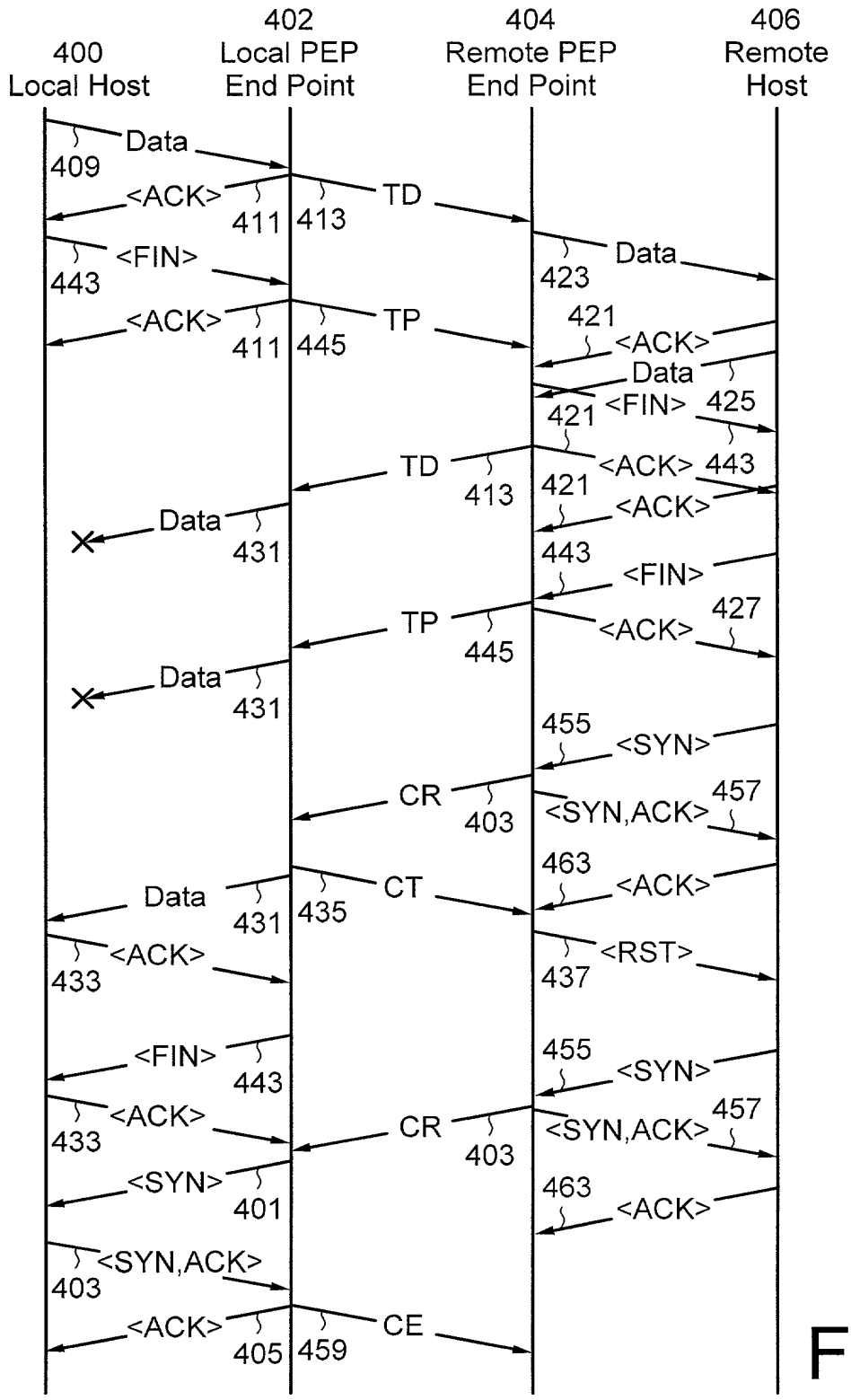

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
Data
409
<ACK>
411
TD
413
Data
423
<FIN>
443
<ACK>
411
TP
445
421
<ACK>
Data
421
<FIN>
425
TD
413
421
<ACK>
443
Data
431
<ACK>
443
<FIN>
TP
445
<ACK>
427
Data
431
455
<SYN>
CR
403
<SYN,ACK>
457
463
Data
431
CT
435
<ACK>
433
<RST>
437
<FIN>
443
455
<SYN>
<ACK>
433
CR
403
<SYN,ACK>
457
<SYN>
401
463
<ACK>
<SYN,ACK>
403
<ACK>
405
CE
459

FIG. 32

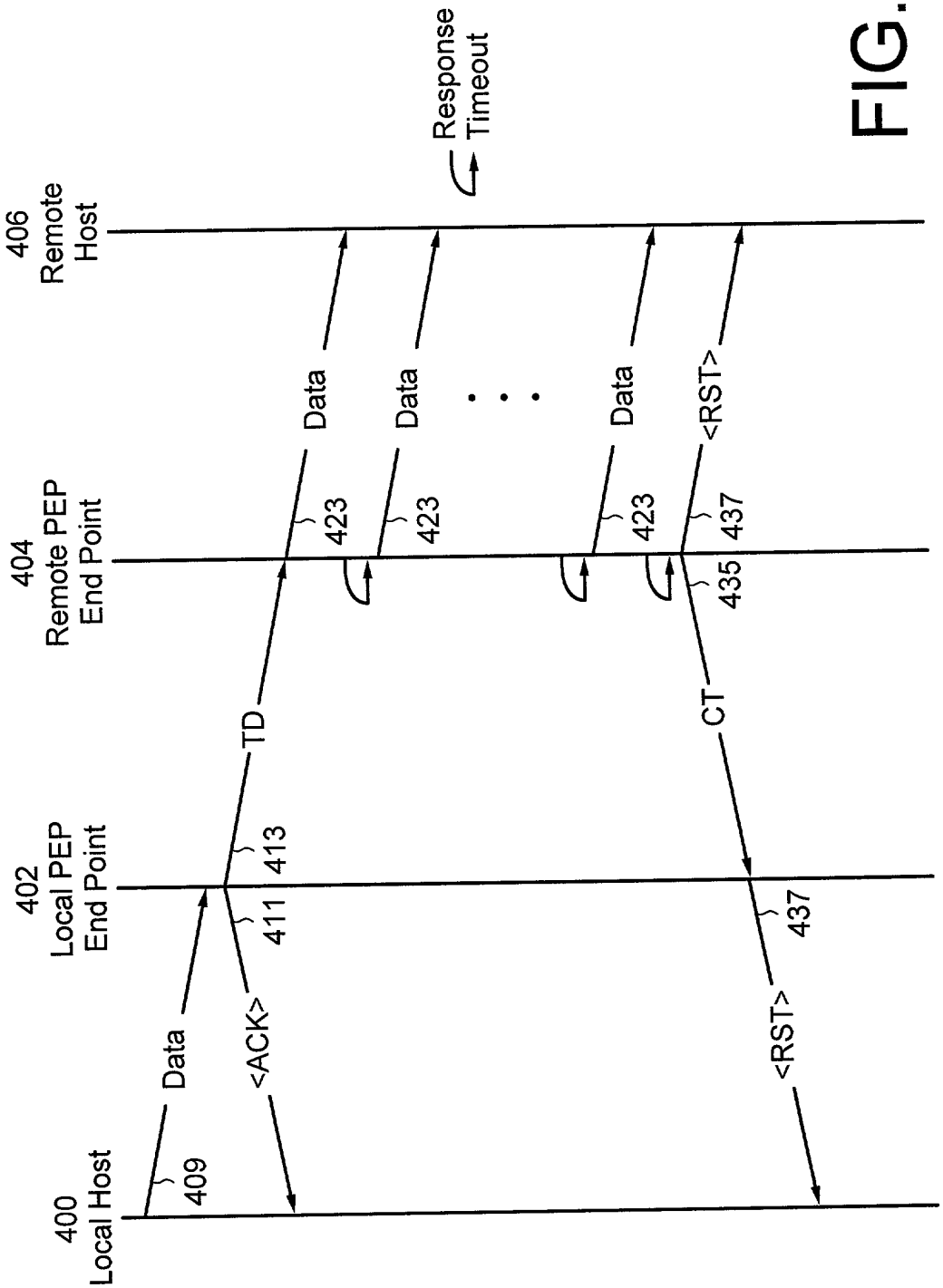

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
Data
409
<ACK>
411
TD
413
Data
423
Data
423
Data
423
Response
Timeout
CT
435
<RST>
437
<RST>
437

FIG. 33

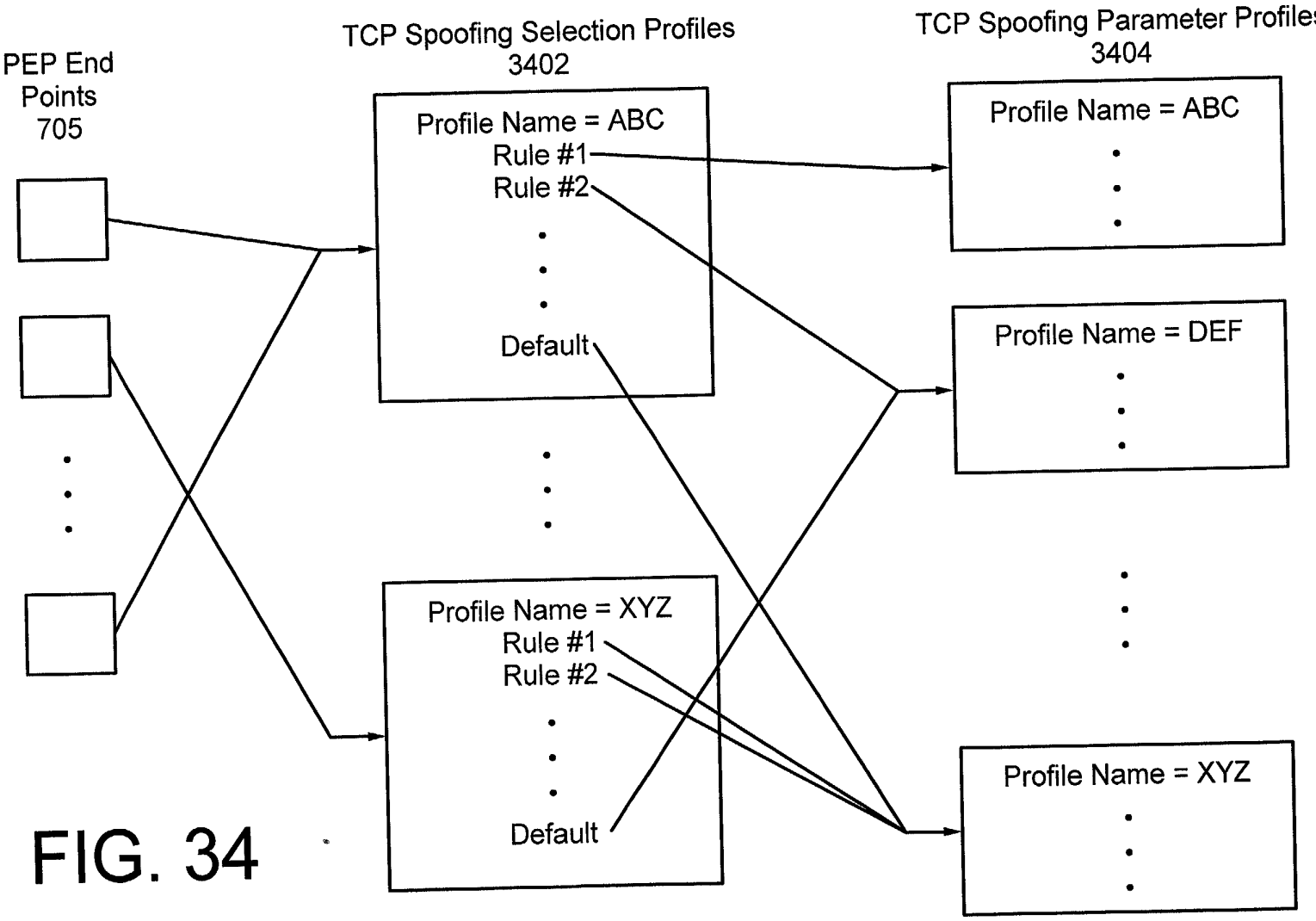

PEP End Points 705
TCP Spoofing Selection Profiles 3402
Profile Name = ABC
Rule #1
Rule #2
Default
Profile Name = XYZ
Rule #1
Rule #2
Default
TCP Spoofing Parameter Profiles 3404
Profile Name = ABC
Profile Name = DEF
Profile Name = XYZ

FIG. 34

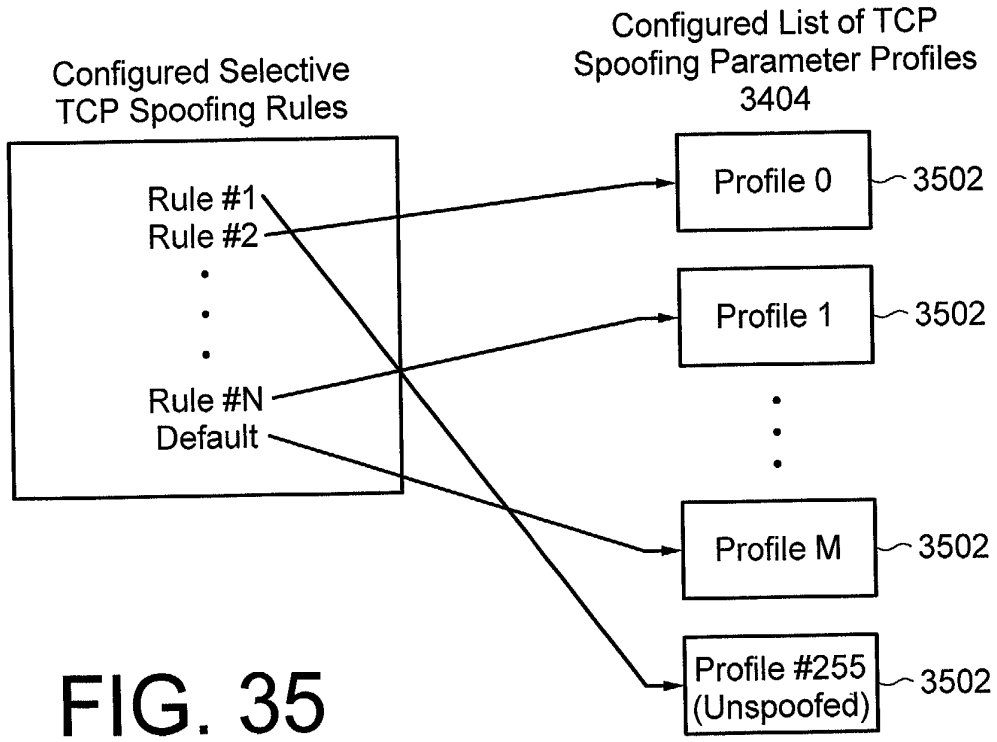

Configured Selective
TCP Spoofing Rules
Rule #1
Rule #2
Rule #N
Default
Configured List of TCP
Spoofing Parameter Profiles
3404
Profile 0
3502
Profile 1
3502
Profile M
3502
Profile #255
(Unspoofed)
3502

FIG. 35

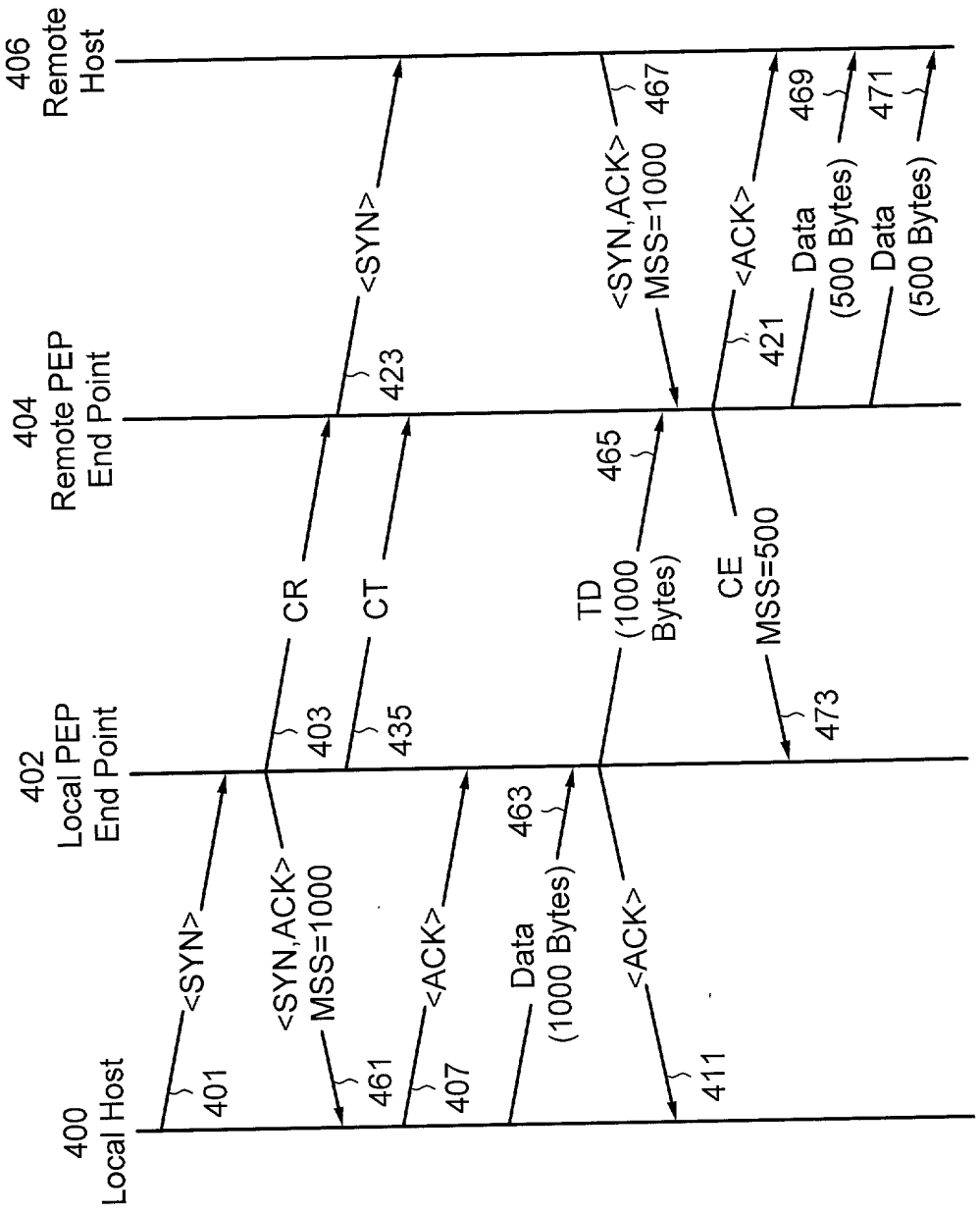

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<SYN>
401
<SYN,ACK>
MSS=1000
461
<ACK>
407
Data
(1000 Bytes)
463
<ACK>
411
CR
403
CT
435
<SYN>
423
TD
(1000
Bytes)
465
CE
MSS=500
473
<SYN,ACK>
MSS=1000
467
<ACK>
421
Data
(500 Bytes)
469
Data
(500 Bytes)
471

FIG. 36

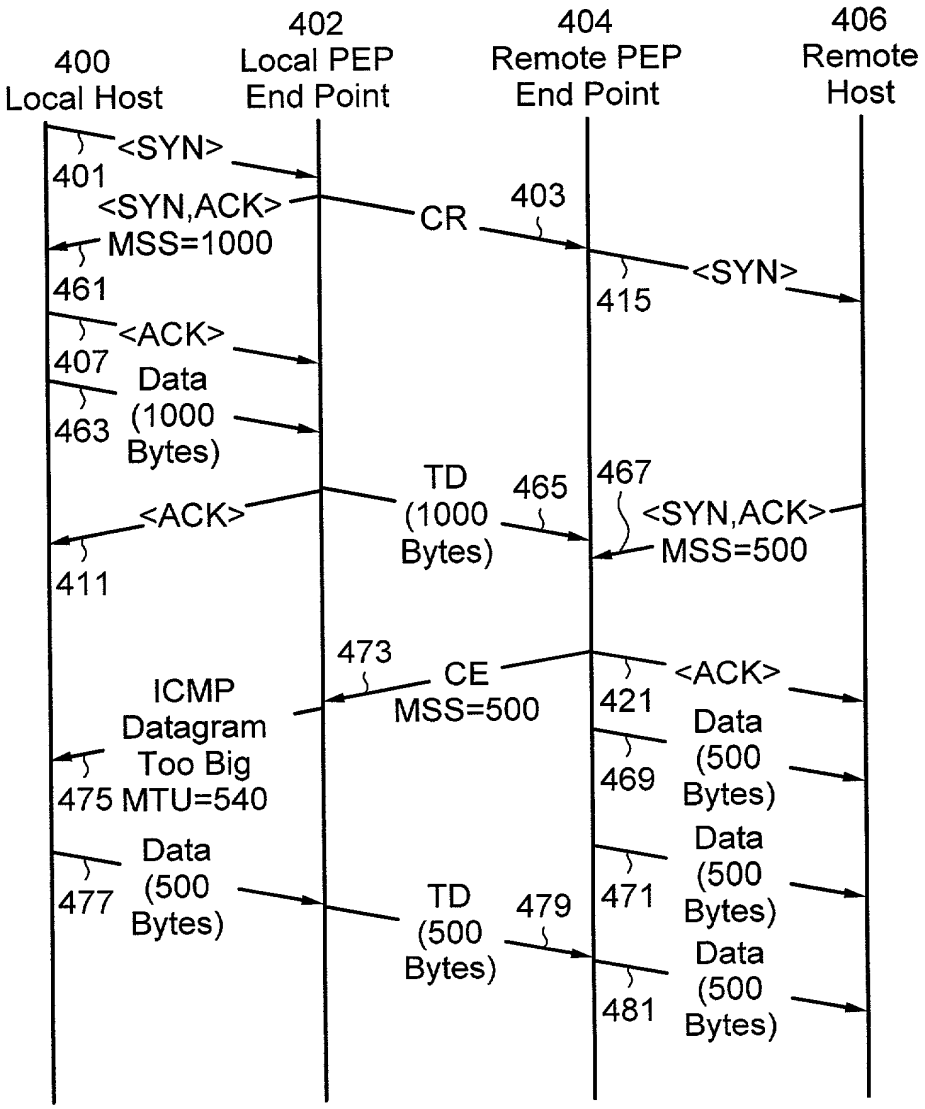

400
Local Host
402
Local PEP
End Point
404
Remote PEP
End Point
406
Remote
Host
<SYN>
401
CR
403
<SYN,ACK>
MSS=1000
461
<SYN>
415
<ACK>
407
Data
(1000
Bytes)
463
TD
(1000
Bytes)
465
467
<SYN,ACK>
MSS=500
<ACK>
411
473
CE
MSS=500
<ACK>
421
ICMP
Datagram
Too Big
MTU=540
475
Data
(500
Bytes)
469
Data
(500
Bytes)
471
Data
(500
Bytes)
477
TD
(500
Bytes)
479
Data
(500
Bytes)
481

FIG. 37

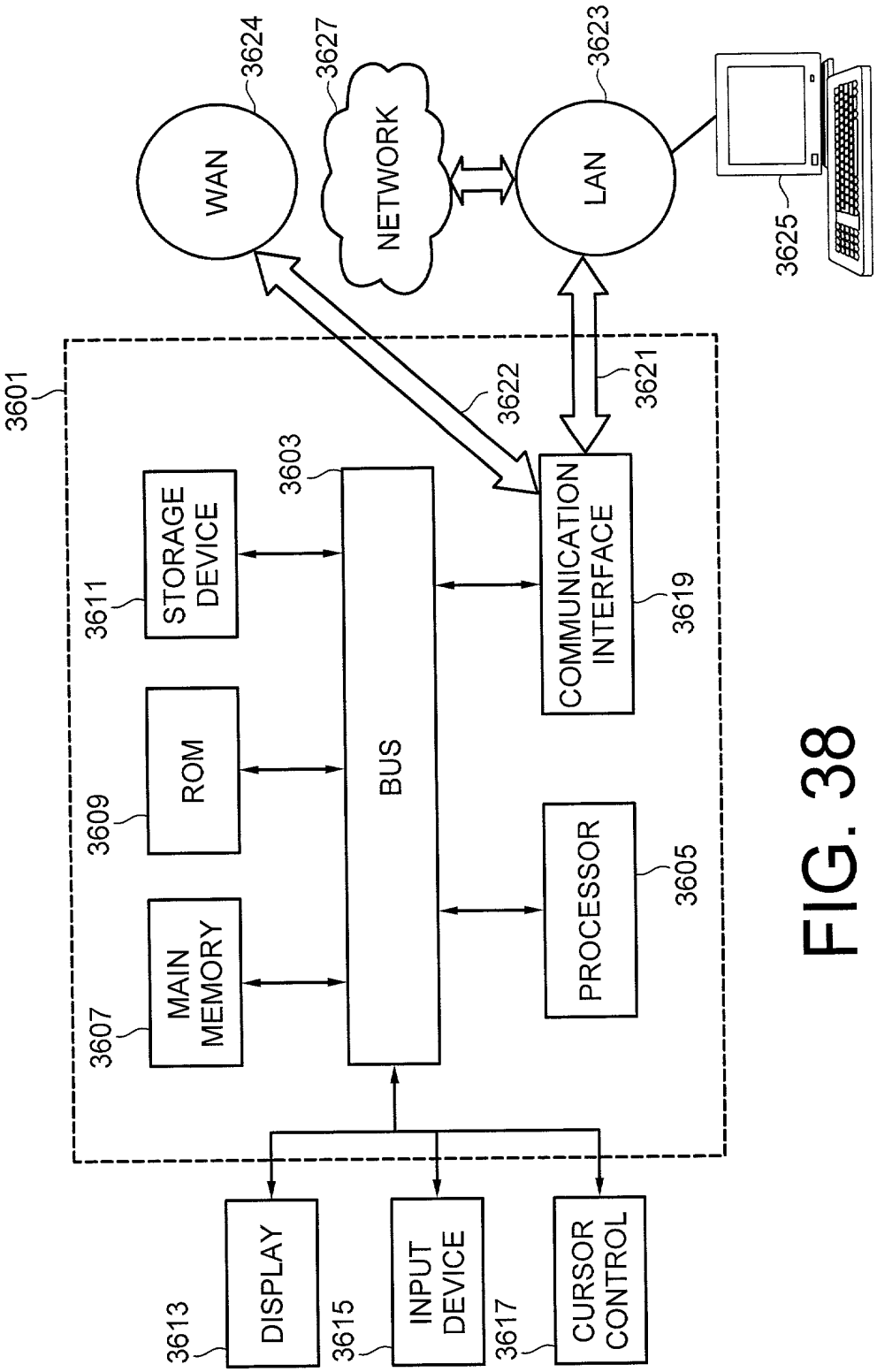

3601
3603
3607
MAIN MEMORY
3609
ROM
3611
STORAGE DEVICE
BUS
PROCESSOR
3605
COMMUNICATION INTERFACE
3619
3621
3622
3623
LAN
3624
WAN
3627
NETWORK
3625
3613
DISPLAY
3615
INPUT DEVICE
3617
CURSOR CONTROL

FIG. 38

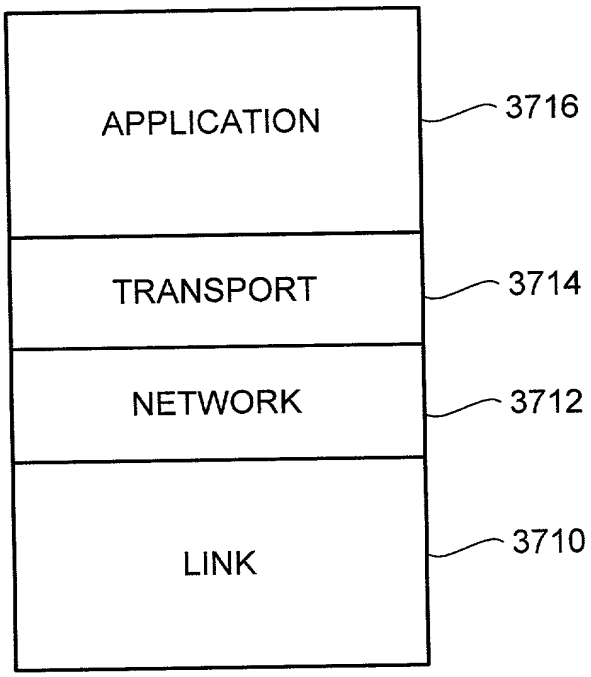
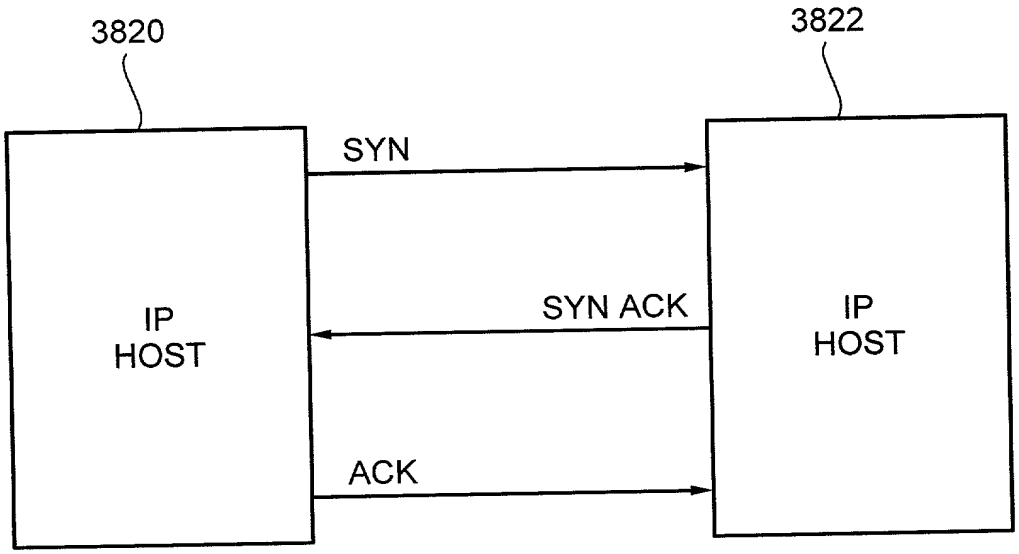


FIG. 39



TCP CONNECTION

FIG. 40